ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

The Costs of an Unnecessarily Stringent Federal Data Privacy Law

ALAN MCQUINN AND DANIEL CASTRO | AUGUST 2019

Federal legislation mirroring key provisions of privacy laws in Europe or California could cost the U.S. economy about $122 billion per year.

KEY TAKEAWAYS

- Federal legislation mirroring key provisions of the European Union's General Data Protection Regulation or the California Consumer Protection Act could cost the U.S. economy approximately $122 billion per year, or $483 per U.S. adult.
- A more focused, but still effective national data privacy law would cost approximately $6 billion per year—around 95 percent less than an EU-style law.
- Overly restrictive privacy rules for the digital economy will increase prices, reduce free access to products and services, and hinder innovation in ways that harm businesses and consumers.
- Congress should enact a targeted federal law to protect consumers, reduce uncertainty and compliance costs for covered organizations, and prevent states from creating a costlier thicket of conflicting laws.

INTRODUCTION

Congress is rightly considering substantial reforms to federal data privacy law. In particular, there is a pressing need to preempt states from subjecting organizations to multiple, conflicting privacy rules. The debate now is not over whether to pass new legislation, but how to design such a law to both protect consumers and encourage continued innovation. Congress must decide whether to model its legislation on the European Union's new data protection law, the General Data Protection Regulation (GDPR), which has imposed significant costs and undermined innovation in the region, or to stay closer to the light-touch approach that has allowed the U.S. digital economy to flourish. This decision will have profound implications for the U.S. economy, as the costs of data privacy laws can be significant. Unfortunately, many proponents of European-style data protection regulations ignore these costs, or even suggest—without convincing evidence—that such legislation would be a net benefit to the U.S. economy.[1] As Congress crafts a new data privacy law, it should understand how decisions about which provisions to include can impact both the direct and indirect costs on businesses and consumers.

The Information Technology and Innovation Foundation (ITIF) estimates that if Congress were to pass legislation that mirrors many of the key provisions in the GDPR or the California Consumer Protection Act (CCPA), it could cost the U.S. economy approximately $122 billion, or $483 per U.S. adult, per year, which is more than 50 percent of what Americans spend on their electric bills each year.[2] In contrast, if Congress passed a more targeted set of privacy protections, it could still boost consumer protection, but reduce costs by 95 percent to approximately $6.5 billion per year.

The costs of regulations can be significant, and are justifiable only when their benefits both outweigh their costs and are achieved in the most cost-effective way. Neither of these are true with regard to the kind of overly restrictive data protection law many privacy advocates have demanded. And even more importantly, Congress can significantly improve data protection for Americans at a fraction of the cost by passing comprehensive data privacy legislation that focuses on a targeted set of reforms. This decision should be easy for lawmakers.

This report evaluates two types of costs associated with a federal data privacy law: compliance costs and market inefficiencies. Compliance costs include personnel companies must hire and capital costs they incur related to new regulations. We analyzed the compliance costs associated with oversight mandates, such as requirements for data protection officers and privacy audits; obligations on organizations to provide certain administrative services and functions to data subjects, such as requirements for data access, portability, deletion, and correction; the impact on productivity for Americans receiving more privacy notices; and duplicative costs associated with an overzealous enforcement regime.

Market inefficiencies are indirect costs that impact organizations by restricting productivity and economic value, including among organizations trying to innovate. For example, there is clear evidence that the ability to effectively analyze data generates economic benefits, while poorly designed privacy laws tend to reduce this economic value.[3] We analyzed the inefficiencies associated with reduced access to data and lower advertising effectiveness.

Finally, Congress should understand that inaction also has costs, especially as many states are considering enacting their own rules, which could be even more costly than overly restrictive federal legislation because of the inefficiency of having no national standard.

Figure 1: Estimate of costs associated with unnecessarily stringent federal data privacy law

Description	Cost
Data Protection Officers	$6,370 M
Privacy Audits	$440 M
Data Infrastructure	$5,380 M
Data Access	$340 M
Data Portability	$510 M
Data Deletion	$780 M
Data Rectification	$190 M
Duplicative Enforcement	$2,710 M
Lower Consumer Efficiency	$1,870 M
Less Access to Data	$71,000 M
Lower Ad Effectiveness	$32,900 M
Total	**$122,490 M**

The United States has multiple federal and state laws that regulate data protection, often focusing on particular sectors or types of data, with multiple regulatory authorities responsible for oversight.[4] However, following the enactment of the GDPR in the EU, a growing chorus of voices is calling for new data privacy laws in the United States.[5] California has already passed the CCPA, and as of June 2019, at least 27 other states have also introduced bills related to data privacy.[6] Now Congress is set to act, too.[7]

Crafting federal data privacy legislation requires a thorough understanding of the direct and indirect implications of various data protection policies. Policymakers who ignore the complexity of complying with data privacy laws or the hidden costs of these regulations risk creating rules that not only lead to significant compliance costs consumers ultimately will bear, but also undermine the digital economy by restricting the overall digital ecosystem and the benefits it provides Americans.[8] For example, the CCPA was rushed into law to head off a worse proposal, leaving legislators, businesses, and consumers without a full understanding of the costs associated with it.[9] CCPA applies to all businesses that have at least $25 million in annual revenue, possess the personal data of over 50,000 consumers, or earn half their revenue from activities related to using personal data.[10] Indeed, lawmakers may not have realized how expansive this definition is: It covers businesses that handle as few as 127 transactions or website visits a day, a trivial number for many businesses.

The costs of the GDPR are much larger. The International Association of Privacy Professionals (IAPP) estimated in 2017 that the Global Fortune 500 alone would spend $7.8 billion in

compliance costs for the GDPR.[11] Another survey of U.S. companies with more than 500 employees found that 68 percent planned to spend between $1 million and $10 million to meet GDPR's requirements.[12] The study found another 9 percent of businesses planned to spend more than $10 million—with over 19,000 U.S. firms having more than 500 employees, total GDPR compliance costs for this group alone could reach $17 billion.[13] Existing U.S. data privacy laws have also proven costly. For example, the Department of Health and Human Services estimated the costs of implementing the privacy portion of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the federal privacy law for health data, would cost $17.6 billion to implement over the first 10 years—although future rule changes would increase these costs.[14] Even relatively minor provisions of privacy laws can quickly add up. For example, the Consumer Financial Protection Bureau estimates that the cost of providing the annual privacy notices associated with the Gramm-Leach-Bliley Act (GLBA) is $12.2 million.[15] To be sure, the cost estimates from these regulatory agencies are likely lower than actual costs borne by covered entities enacting the rules, and do not include downstream inefficiencies in the economy that may result from decreased use of data. Unfortunately, many of those advocating for new data privacy laws either ignore the costs of new regulations, falsely claim all costs will simply come out of corporate profits (as if that were a justification for the high costs), or wrongly assume greater digital adoption from the law will outweigh the costs.[16]

Congress can and should do better. If the only goal of data privacy legislation were to increase consumer privacy, then Congress could ignore costs. But the goal of any social or economic regulation, including data privacy legislation, is to maximize consumer welfare, of which privacy is just one component. Maximizing consumer welfare requires accounting for costs, because expensive rules increase prices (or reduce free access to products and services) and hinder the development of improved products and services. Federal data privacy legislation should not be a hidden tax on consumers.

METHODOLOGY

This report highlights two major categories of costs associated with a poorly designed federal privacy regulation—compliance costs and market inefficiencies—and describes several different types of regulations that incur these costs. Due to a lack of specific data and studies, some estimates are merely back-of-the-envelope attempts to predict difficult-to-measure elements of regulatory compliance. Moreover, this list of costs is not exhaustive, as the impact of certain effects, such as generating uncertainty for organizations, is harder to estimate. Each of our estimates for compliance costs—which we intentionally kept conservative—assumes the costs were new and companies were not already hiring labor or building infrastructure to tackle these problems.[17] Each section explores the metrics we assessed in order to reach our conclusions.

Importantly, we attempted to measure these costs and inefficiencies for all types of non-governmental organizations that could be impacted by regulatory compliance, including both for-profit and nonprofit entities. While some privacy laws, such as the CCPA, have excluded nonprofit entities or limited exposure for small businesses, other laws, such as the GDPR, have included every type of organization that handles personal information. It is still to be determined whether a federal privacy law in the United States will carve out exemptions for specific entities or businesses. Indeed, while some proposals have targeted certain entities with exact thresholds for their number of consumers or amount of revenue, such as Sen. Ron Wyden's (D-OR)

Consumer Data Protection Act, others, such as Sen. Marsha Blackburn's (R-TN) BROWSER Act, are broadly drafted so as to cover every type of service offered over the Internet.[18] Therefore, we assessed costs for all types of entities and attempted to break them down for specific entities to provide as much utility in these estimates as we could, with topline estimates including costs to both for-profit and nonprofit entities. Finally, while related to regulatory costs on organizations, we estimated direct costs for U.S. consumers in the form of excess time spent addressing the new regulations (e.g., privacy notices).

Moreover, these estimates do not consider the costs associated with different jurisdictions creating conflicting standards for data privacy. For example, if Maine and California require different standards for obtaining consent or providing data portability, an organization operating in both would be subject to higher costs than if the two states had identical privacy regimes. As such, if a federal privacy bill fails to preempt states from creating a regulatory patchwork, costs will be even higher than the estimates within this report.

COMPLIANCE COSTS

When companies are required to devote resources to regulatory compliance, they usually either reduce investment in improving existing products and services or developing new ones, or pass at least a portion of the costs on to consumers, depending on the competitive nature and price elasticity of each market. If the United States were to pass stringent federal privacy legislation, **U.S. organizations and consumers would spend up to $18 billion annually in compliance costs.** These costs would increase if both the federal data protection law did not fully preempt state and local legislation, and organizations of all sizes had to comply with all federal requirements. This cost is hard to estimate and would change depending on the number of state laws and provisions included therein. But because the provisions would be in addition to new federal rules, they would increase compliance costs.

This report analyzes compliance costs associated with several components of data privacy legislation: data protection officers; privacy audits, improving data quality to facilitate subject requests, costs associated with four types of potential user rights (access, data portability, deletion requests, and data correction—also called data rectification), the costs of increased legal risk and duplicative enforcement, and productivity costs for consumers as a result of pop-up consent notices.

Data Protection Officers

Some data privacy laws require organizations to designate a data protection officer to be responsible for compliance. These laws create direct costs either by requiring organizations to hire additional personnel to handle consumer privacy requests, system upkeep, and regulatory compliance, or by requiring existing personnel to divert their time from other activities.

The cost of requiring data protection officers for all U.S. organizations that handle personal data would be roughly $6.4 billion annually.

The GDPR requires organizations to have a data protection officer or other accountable individual to guarantee compliance with the law. It covers businesses of all sizes and all sectors, as virtually all firms collect personal data, such as data about their employees, customers, and visitors to their website. Depending on the scope and definition of the covered entities, a potential federal privacy law could impact a significant portion of organizations in the United States. Some

organizations may hire consultants to help manage their requirements under the law. Others, especially those with many complex systems that handle personal data, may hire several internal data protection officers to solely handle compliance. Some, especially those with a small amount of personal information, may simple delegate the task to current employees.

We accounted for this variation in employment in two ways. First, we tried to ascertain the likely number of for-profit and nonprofit organizations that would need to hire data protection officers. To estimate this, we used accountants and bookkeepers as a benchmark. Only 22 percent of small businesses employed a full or part-time accountant or consultant in 2018.[19] To keep our estimates conservative, we discounted this number by over half based on the fact that not every company needs a data protection officer. Therefore, we estimate that at least 10 percent of small businesses (fewer than 20 employees) would be required to hire data protection officers. Medium-sized and large businesses are much more likely to hire accountants, whether consultants or in-house personnel, to handle their increasingly complex financial systems.[20] With regard to privacy compliance, the larger the organization the more likely they are to need individuals to help with data protection compliance. Therefore, we estimate at least 25 percent of medium-sized businesses (20 to 500 employees) and 50 percent of large businesses (more than 500 employees) are likely to hire these personnel.[21] Finally, nonprofits will also need to hire data protection officers in order to fulfill their requirements under the law. We estimate that nonprofits will hire full-time data protection officers or part-time consultants at roughly the same rate as small businesses. Therefore, at least 10 percent of nonprofits could be required to make these additional hires.

Second, we estimated how many data protection officers each business would be likely to actually hire, once again using accounting and bookkeeping as a metric. A survey by the Institute of Certified Bookkeepers found that half of the respondents had fewer than 20 clients.[22] We used this as the metric for the number of small businesses a data protection officer could serve, and concluded small businesses will need to hire the services of 0.05 data protection officers, which represents 1 data privacy officer for every 20 businesses. Again, medium-sized and large businesses would be more likely to hire both bookkeepers (or accountants) and data protection officers. Therefore medium-sized businesses would need to hire the services of 0.1 data protection officers, or 1 officer for every 10 businesses, and large businesses would likely need to hire 1 data protection officer each. Here again, nonprofits would hire data protection officers at the same rate as small businesses, or roughly 0.05 data protection officers per nonprofit. These are average, conservative estimates per organization based on the above assumptions, and may significantly change depending on the scope of the law (or laws).

Given there are roughly 5,300,000 small businesses, 616,000 medium-sized businesses, and 19,000 large businesses in the United States, federal legislation could result in U.S. companies needing to hire the equivalent of roughly 51,000 data protection officers.[23] In addition, according to the National Center for Charitable Statistics, there are roughly 1.56 million nonprofit organizations registered in the United States.[24] By the metrics discussed above, U.S. nonprofits would need to hire the equivalent of roughly an additional 8,000 data protection officers.

For the cost of these for-profit and nonprofit employees, we used the average annual salary of privacy officers in the United States as reported by Glassdoor.[25] This figure is $77,000 per year.

In addition to salary, there are overhead costs. For example, businesses pay for benefits, overhead, fringe costs, taxes, administrative costs, and physical space to support new hires. We used government contractors as a benchmark because they must account for these costs and submit to transparency reporting and audits, using a multiplier called a "wrap rate."[26] According to a 2017 survey of government contractors, the range of wrap rate multipliers for costs associated with having workers at government locations is between 1.4 and 2.3.[27] We used the lower end of the range of these wrap rates to ensure our estimate was conservative, selecting a multiplier of 1.4 to account for overhead labor costs. Therefore, each new data protection officer would cost an organization an average of $108,000 per year, and likely cost U.S. businesses and nonprofits roughly $6.4 billion annually.

Figure 2: Costs associated with hiring privacy personnel

Type of Organization	# of DPOs	$ per DPO	Cost
Small businesses	26,000	$108,000	$2,810 M
Medium-sized businesses	15,000	$108,000	$1,620 M
Large businesses	10,000	$108,000	$1,080 M
Nonprofits	8,000	$108,000	$860 M
Total			**$6,370 M**

Privacy Audits

Some privacy laws require organizations to submit to periodic compliance audits, administered by either their organization or a third party. For example, the GDPR requires organizations to demonstrate compliance by participating in periodic audits—and even direct inspections—by data protection authorities.[28] While exact audit numbers under the GDPR do not exist, the majority of GDPR-covered organizations expected to be subject to a compliance audit before it went into effect.[29] Data protection authorities have released certain audit details post-enforcement. For example, the Swedish DPO reviewed 350 companies and authorities as part of its first wave of audits in October 2018.[30] Similarly, HIPAA requires its covered entities and their business associates to meet selected standards and implementation specifications, which they must periodically prove through comprehensive privacy and security audits.[31] Several proposed federal privacy bills also incorporate such an audit provision.[32] Privacy audits are not usually required on a set timeframe, but rather are at the discretion of the organizations.

The cost of requiring privacy audits for all U.S. organizations that handle personal data would be roughly $440 million.

Audit requirements will likely affect different types of businesses in different ways, based on the types of data they collect and the protections required in the law. Audits will likely be required, for example, after a data breach, series of complaints, or random inquiry from a regulator. Only 0.5 percent of organizations annually will likely need to do a full audit.[33] To estimate this cost, we used HIPAA compliance as a benchmark. According to the health care compliance company Datica, a full HIPAA audit costs between $30,000 and $60,000 for both employee and direct costs.[34] And to ensure a conservative estimate, we calculated small businesses and nonprofits

will spend $10,000 per audit, while medium-sized companies will spend the lower end of HIPAA's full audit cost thresholds ($30,000), and large companies the higher end of HIPAA's full audit cost thresholds ($60,000).

Figure 3: Costs associated with privacy audits

Type of Organization	# of Audits	$ per Audit	Cost
Small businesses	26,000	$10,000	$260 M
Medium-sized businesses	3,000	$30,000	$90 M
Large businesses	100	$60,000	$6 M
Nonprofits	8,000	$10,000	$80 M
Total			**$440 M**

Right to Access, Deletion, Data Portability, and Rectification

Privacy laws often give users a set of rights. These rights can include the right to access personal data stored by an organization, port that data to other services, delete that data, and make corrections to that data.

Privacy rights that allow users to make a direct request from a company will come with three types of costs. First, companies will need to build and maintain data infrastructure they can easily query in order to store, find, and update the requested personal information. The compliance costs associated with creating this data infrastructure include initial development and deployment costs and maintenance costs. Costs associated with this category occur no matter which rights a privacy law creates, but are not compounded for each set of rights. For example, if a privacy law creates both a right of access and a right of deletion, organizations will only need to build the data infrastructure once in order to comply with both types of requests.

Second, businesses will need to create a mechanism to verify and authenticate users are who they say they are. Authentication is important. Without proper authentication protocols, privacy laws that enable users to access their data, delete it, or port it to other services can actually increase the "attack surface" of personal data by enabling additional access points for bad actors to exploit.[35] For example, a malicious actor could hack into a user's Spotify account that uses Europe right-of-access privacy rights to request a file with all of the account holder's data.[36] Authentication tools can be as simple as a user name and password for online services that already have the infrastructure, or as complex as third-party authentication services that utilize government identification to establish identity. The costs are smaller for the former and larger for the latter, but both can be quite significant for businesses. One report from the Fido alliance found that businesses that authenticate their customers spend an average of $307,000 annually on authentication costs.[37]

Finally, each of these rights will come with processing costs, which vary based on the specific request. Most of these requests will likely come through digital portals, although because of a lack of digital literacy and access to Internet service, businesses will still need to receive and process some requests over the phone, by mail, or in person. This type of human processing can increase costs significantly. Indeed, a 2014 report found that between 20 and 50 percent of all

help desk calls were for authentication problems (e.g., password resets)—the average labor cost of which was about $70 in 2014.[38]

The following will attempt to establish an average for each estimate.

The total cost of providing a right to access, deletion, data portability, and rectification will be $7.2 billion.

Update and Maintain Data Infrastructure

While collecting and storing data may be getting cheaper, creating and maintaining high-quality data still can be costly.[39] Companies may have databases that can neither communicate with one another nor collect data that is improperly formatted, lacks metadata, or is incorrect or incomplete. In a survey of 75 companies, only 3 percent had data that met basic quality standards.[40]

To ensure data quality, previously collected personal information that exists on an organization's servers must be properly coded to track personal information, while new inputs must be in the proper format. Ensuring data quality and searchability within organizations' infrastructures will require employees—data analysts, database administrators, and engineers—to ensure fulfillment. These costs will likely be different for start-ups and newer businesses, which can build the necessary systems from the outset, as opposed to businesses that will need to update legacy systems in order to be compliant.

The cost of updating and maintaining data infrastructure for all U.S. companies that handle personal data would be roughly $5.4 billion.

To ensure organizations are able to track, access, correct, and delete personal data in their systems, they will need to hire data analysts or database administrators to build and maintain data infrastructure. Given data scientists typically spend 80 percent of their time cleaning and preparing data to make it usable, it is likely many companies will need to hire staff whose primary goal will be to maintain data quality.[41] Some companies may also hire consultants to help manage their requirements under the law. Others, especially those with complex management systems that handle personal data, may hire several data analysts to clean up and maintain their data infrastructure. The distinction between small and large businesses is less relevant for digital businesses with few employees that serve large numbers of customers.

We used the same metrics for small businesses as nonprofits, using accounting as a baseline for our estimate for small businesses, and then scaling that estimate for medium-sized and large businesses. However, because larger-scale organizations are more likely to facilitate user requests, we increased our estimates slightly for medium-sized and larger businesses with respect to data analysts. Therefore, conservatively, we believe 10 percent of small businesses and nonprofits, 25 percent of medium-sized businesses, and 50 percent of large businesses would need to hire data analysts or database administrators to maintain data quality. While many of these organizations will have direct hires to manage their data infrastructure, some may hire outside firms to do so. We predict small businesses falling within this category will need to hire an average of 0.05 personnel, medium-sized businesses will need to hire the services of an average of 0.1 new workers, and large businesses will need to hire an average of 1 worker. This represents the equivalent of 1 database analyst or database manager for every 20 small

businesses and nonprofits, 1 for every 10 medium-sized businesses, and 1 for every large business, respectively—the same ratios we used for data protection officers.

According to Glassdoor, the median salary of an entry-level data analyst or database administrator is roughly $65,000.[42] To account for overhead costs, we used the multiplier of 1.4 (discussed in detail in the section on data protection officers), for a per-worker cost of $91,000. With 51,000 businesses and 8,000 nonprofits needing to hire personnel to clean their data, the costs associated with updating and maintaining data infrastructure will be $5.4 billion.

Figure 4: Costs associated with updating and maintaining data infrastructure

Type of Organization	# of DAs	$ per DA	Cost
Small businesses	26,000	$91,000	$2,370 M
Medium-sized businesses	15,000	$91,000	$1,370 M
Large businesses	10,000	$91,000	$910 M
Nonprofits	8,000	$91,000	$730 M
Total			**$5,380 M**

Importantly, it is likely the labor market for data professionals is insufficient to provide the number of these positions needed to fulfil this requirement across the United States, so organizations may pay a premium.

Data Access

Some privacy laws require organizations to provide individuals, on request, a copy of their personal data and other supplementary information. These provisions, called the "rights of access," typically state whether organizations may charge for this access, and how long they have to respond to requests. For example, the GDPR and CCPA both create subject access rights free of charge—and several proposed federal bills have sought to create these rights for individuals requesting their information from certain entities in the United States.[43]

The cost of unbounded access requirements for all U.S. organizations that handle personal data would be $340 million annually.

User access requests will depend on the type of organization and the number of users it serves. Since the GDPR went into effect, patients have made roughly 140 requests per doctor annually.[44] Large financial services companies, on the other hand, receive as many as 11 million requests per year as a result of European regulations.[45] Some individuals may even "weaponize" access requests to intentionally raise compliance costs for the companies involved.[46] Therefore, the number of requests an organization receives can vary wildly based on the amount of information it processes, the number of individuals it serves, the utility of the data, and other factors.

To ascertain how many access requests companies might receive under a federal law, we first estimated the number of online accounts the average U.S. adult holds. The United States has 238 million Internet users over the age of 14, and the average U.S. Internet user has 130 online accounts.[47] Therefore, U.S. consumers have roughly 31 billion online accounts. Some of these

accounts are for services that are much more likely to elicit access requests, such as banking, credit cards, health care, utilities, social media, and email. Therefore, we assume only a small fraction of these accounts (5 percent, or 1.5 billion accounts) will involve these high-impact online services.[48] We conservatively conclude 25 percent of U.S. consumers will make access requests for these accounts based on the fact that, in 2018, 38 percent of U.S. consumers reported obtaining their credit report sometime during the previous year.[49] Using these figures, we predict high-impact online activities will receive roughly 387 million requests each year.

We put all other online accounts, such as entertainment sites and retailers, into the category of "low-impact online activities," which equals roughly 29 billion online accounts. We expect these services to receive significantly fewer requests (only 1 percent, or roughly 294 million requests). Based on these assumptions, we believe U.S. organizations would receive roughly 681 million access requests each year, or an average of 2.7 per U.S. adult.

Once an organization's systems are optimized for searchability and to handle requests, there are two primary costs associated with providing access to records: user authentication costs and processing costs. First, authentication costs can be very high for businesses. For example, one third-party digital identification company lists basic authentication services (not including multifactor authentication) as $2 per user per month, while another lists these fees as $0.27 per user per year.[50] To keep our estimate conservative, we used authentication costs to be $0.25 per record for each request. Given 681 million requests, we calculated the annual costs associated with verifying users as $170 million.

Processing costs are those associated with complying with user requests to process data for individuals. We used costs associated with providing free credit reports and scores, due to requirements in the Fair and Accurate Credit Transactions Act, as a benchmark. Credit reporting agencies in the United States charge consumers roughly $2.50 to $8 for a single set of records.[51] Similarly, for credit score reporting—which is less demanding than most right-of-access proposals—one credit bureau estimated FICO-score acquisition costs of between $0.05 and $0.15 per score.[52] Given these estimates, it is reasonable to assume a comparative figure for the costs associated with providing users with similar access to data is roughly $0.25 per request. Therefore, we estimated the processing costs of unbounded access requirements to be $170 million annually. Importantly, this figure does not consider maintenance or upkeep costs for these systems.

Therefore, the total cost of subject access requests would be $340 million.

Figure 5: Costs associated with data access requirements

Description	# of Requests	$ per Request	Cost
Verification	680 M	$0.25	$170 M
Processing	680 M	$0.25	$170 M
Total			**$340 M**

Some of the costs associated with providing access to users can be mitigated by allowing organizations to recover reasonable cost for processing requests. This would enable them to

recoup some costs and deter users from launching excessive requests for data that is of limited utility.

Data Portability

Data portability is a specific type of right of access that requires organizations to provide consumers with a copy of their data in a machine-readable format. One goal of data portability provisions is to allow consumers to both obtain a copy of their personal information as well as provide their personal information to a competing service. Several privacy laws, including the GDPR and HIPAA, include data portability requirements. According to IAPP, data portability ranks among the most difficult compliance obligations for privacy laws.[53]

Data portability requires organizations to provide data in a standard format, through either a direct download or an open application programming interface (API)—a set of functions and procedures developers can use to access the features or data of an operating system, application, or other service. In this case, APIs enable third parties to access consumer information directly from a service when users request their data be ported to that third party.[54]

The cost of data portability requirements for all U.S. organizations that handle personal data would be roughly $510 million.

Similar to the access request estimate, we estimate that a certain threshold of online accounts will be in high-impact online activities that are more likely to elicit data portability requests (e.g., online banking, credit cards, utilities, email, etc.). We assume only a small fraction of these accounts (5 percent, or 1.5 billion) will involve these high-impact online services.[55] We conservatively conclude that 25 percent of U.S. consumers will make access requests for high-impact accounts based on the fact that, in 2018, 38 percent of U.S. consumers reported obtaining their credit score sometime during the previous year.[56] Using these metrics, we predict high-impact online activities will receive roughly 387 million data portability requests each year.

We put all other online accounts, such as entertainment sites and retailers, into the category of "low-impact online activities," which equals roughly 29 billion online accounts. We expect these services to receive significantly fewer requests (only 1 percent, or roughly 294 million requests). Based on these assumptions, we believe U.S. organizations would receive roughly 681 million data portability requests each year, or an average of 2.7 per U.S. adult.

There are two primary costs associated with organizations providing data portability: user authentication costs and processing costs. We predict authentication costs will average $0.25 per record per request. Given 681 million requests, the costs associated with verifying users would be $170 million annually.

Processing costs are per-request costs associated with complying with user requests to process data for individuals. These costs differ widely based on the needs of any particular business. For example, an organization with 100 requests per week may need to set up a specialized platform for users by providing data in a standard format, either through a direct download or through an open API. This would create additional costs. One 2014 study from the United Kingdom's Open Data Institute, which focuses on open banking regulations in the United Kingdom, found that costs tended to be "below £1m, and tended to cluster in the low-to-mid hundreds of thousands [of pounds per bank]."[57] On the other hand, a business that receives a single request each month may choose to handle them over the phone, with higher costs per request but negligible costs

overall. To keep our estimate conservative, we calculated average processing data portability requests will cost roughly $0.50 each. Given 681 million requests, we estimate the costs associated with verifying users as $340 million annually

Therefore, the costs associated with organizations with personal data creating data portability requirements could be a roughly $510 million annually in the United States.

Figure 6: Costs associated with data portability requirements

Description	# of Requests	$ per Request	Cost
Verification	680 M	$0.25	$170 M
Processing	680 M	$0.50	$340 M
Total			**$510 M**

Moreover, similar to access requirements, some of the costs associated with data portability can easily be mitigated by allowing organizations to charge small amounts for processing requests, particularly those related to large, old, complex, and non-digitized data sets.

Data Deletion

The right to deletion requires data controllers to, on request by data subjects, delete data. Some laws obligate organizations to irrevocably delete the information, while others allow for the data to be recovered by the data controller. For example, the GDPR gives users the right to delete their information.[58] Similarly, the CCPA gives consumers the right to delete any personal information a provider has collected.[59]

The cost of data deletion requirements for all U.S. organizations that handle personal data would be roughly $780 million each year.

We do not believe certain industries or applications will illicit deletion requests higher than other industries. Therefore, online accounts represent those of nonprofits, small businesses, medium-sized businesses, and large businesses of all levels of impact. To establish how many of these accounts users will delete each year (out of 31 billion), we looked to surveys of start-ups that self-reported customer churn rates (i.e., the rates of attrition of customers from services). One survey found that 44 percent of companies had churn rates of between 3 and 7 percent, while 30 percent reported churn rates of over 15 percent.[60] To ensure our estimate was conservative, we used an annual churn rate of 5 percent. Given these assumptions, U.S. consumers will delete roughly 1.5 billion accounts, or roughly 6.1 requests per U.S. adult, annually.

There are two primary costs associated with organizations deleting data: user authentication costs and processing costs. We predict authentication costs will average $0.25 per record per request. Processing costs are per-request costs associated with complying with user requests to delete data for individuals. Once organizations become able to maintain high-quality data and create a process for deleting that data, the processing costs will be negligible for data deletion requirements. However, there are also processing costs associated with creating and maintaining a functional mechanism to delete information after it has been located. To keep our estimate conservative, we calculated that, on average, setting up a means of facilitating data portability

requests will cost roughly $0.25 each. Given 1.5 billion requests, both the authentication and processing costs associated with deletion requests will be $390 million each annually.

Therefore, we estimate that the cost associated with organizations with personal data creating data deletion requirements could be a roughly $780 million annually in the United States.

Figure 7: Costs associated with data deletion requirements

Description	# of Requests	$ per Request	Cost
Verification	1,550 M	$0.25	$390 M
Processing	1,550 M	$0.25	$390 M
Total			**$780 M**

Data Rectification

The right to rectification requires organizations to, on request, correct information in their databases that is inaccurate. Several privacy laws enable users to correct information, including the GDPR and the Family Education Rights and Privacy Act, which regulates privacy protections for education data in the United States.[61] Similarly, credit laws often allow users to correct errors in their credit histories in order to help them avoid harms that would result from erroneous credit information.

The cost of rectification requirements for all U.S. organizations that handle personal data would be roughly $190 million.

We believe a certain threshold of online accounts will be in high-impact online activities that are more likely to elicit rectification requests (e.g., online banking, credit cards, utilities, email, etc.). We assume only a small fraction of these accounts (5 percent, or 1.5 billion accounts) will involve these high-impact online services. We conclude that users of high-impact services will only exercise their right to rectification on 8 percent of the accounts based on an equivalent percentage of U.S. consumers seeking to correct their credit reports.[62] Using these metrics, we believe high-impact online activities will receive roughly 123 million correction requests each year.

We put all other online accounts into the category of "low-impact online activities." These services are significantly less likely to receive such requests. We assume only users of low-impact services will seek to correct data on 0.1 percent of these accounts based a similar percentage of European Internet users exercising their right to be forgotten with Google.[63] This comes to roughly 29 million requests. Given these assumptions, U.S. businesses will receive roughly 150 million correction requests, or roughly 0.6 requests per U.S. adult, each year.

There are two primary costs associated with organizations enabling users to correct data: user authentication costs and processing costs. We predict authentication costs will average $0.25 per record per request. Given 150 million requests, we estimate the costs associated with verifying users as $40 million annually.

Processing costs are per-request costs associated with complying with user requests to correct data for individuals. Unlike access, data portability, and deletion requests, it is more difficult to

create mechanisms to automatically fulfill correction requests. Moreover, there are processing costs associated with creating and maintaining a functional mechanism to correct information after it has been located. Organizations that receive more requests each month may need to create a dedicated portal for users to easily access and update their information, while organizations that receive negligible requests may choose other avenues for fulfilment, such as handling those requests over the phone. Therefore, we calculate the average cost associated with rectification requests will be roughly $1 each, for a total of $150 million annually.

The cost of ensuring all businesses with personal data create data deletion requirements could be a roughly $190 million annually in the United States.

Figure 8: Costs associated with data rectification requirements

Description	# of Requests	$ per Request	Cost
Verification	150 M	$0.25	$40 M
Processing	150 M	$1.00	$150 M
Total			**$190 M**

Costs of Duplicative and Frivolous Enforcement

Enforcement is important because it enables regulators to have oversight over organizations while ensuring they are held accountable when they do not follow the rules. However, enforcement mechanisms in privacy laws, if not carefully considered, can create duplicative enforcement efforts that unfairly generate high costs for organizations. Indeed, if both regulators and private parties can pursue cases for identical reasons, firms can be tied up in lawsuits for years and pay hefty fees for each incident. Importantly, many organizations and lawmakers have proposed duplicative enforcement regimes.

Most privacy laws enable government regulators to enforce their rules. For example, the CCPA instills the California Attorney General with the power to enforce its provisions. Moreover, there can also be general privacy regulators that uphold enforcement. For example, in the United States, the Federal Trade Commission (FTC) is the primary regulator for consumer privacy through its authority to take action against organizations that engage in "unfair or deceptive practices."[64] Basically, when organizations do not keep their promises to protect consumer data, the FTC can pursue enforcement actions against them.

Privacy laws can also enable users to sue a company directly for civil penalties, which is known as private right of action, if that company violates the framework. Private right of action substantially increases companies' legal risks, which inevitably leads to unnecessary lawsuits, some of which are initiated by plaintiffs' lawyers. For example, a vague Illinois law that allows consumers to sue organizations for using facial recognition technology without their permission has resulted in several significant, but largely groundless, class-action lawsuits against such tech companies as Facebook, Shutterfly, and Snapchat.[65] Lawyers may be happy with extraneous lawsuits, but consumers will ultimately pay the price, as organizations are forced to spend money on duplicative and often frivolous lawsuits, rather than investing it in other areas, such as by lowering prices, offering discounts, or creating new products and services.

The average cost of duplicative enforcement mechanisms for all U.S. organizations that handle personal data would be between roughly $2.7 billion if federal law enabled universal private right of action.

These privacy laws are often drafted in a way that exposes organizations—of all sizes—to heightened legal risk, as most firms collect data about their employees, customers, and visitors to their websites. For example, the GDPR applies to all businesses and nonprofits handling any type of personal data.[66] Laws such as the GDPR and CCPA enable both consumers and government regulators to seek civil damages for violations. Fortunately for organizations covered under those acts, violations that result in enforcement actions are relatively rare. Importantly, this section only accounts for costs to society from duplicative enforcement mechanisms and does not consider fines. It is important that regulators have the means with which to hold organizations accountable for privacy and security violations.

While privacy laws can be very broadly drafted to cover many different entities, the actual oversight of these rules can be difficult. There are a limited number of regulators to bring enforcement actions in a large pool of businesses that may not necessarily comply. Moreover, most lawyers are unlikely to take up private right of action cases unless the cases involve a large number of individual violations—bigger cases deliver bigger fees. For example, a lawyer is unlikely to take up the case of a business failing to follow through on only a single deletion request, because the legal fees would dwarf the minimal amount of potential statutory damages. They are much more likely to represent multiple plaintiffs in a suit that results in the release of information from many different potential clients.

There will be both federal and state enforcement actions. For the purposes of this report, we assume federal data privacy legislation vastly expands the enforcement abilities of the FTC, which is the primary consumer protection regulator in the United States, as well as enables states to bring individual (or joint) enforcement actions on their own. In a 2018 report, the FTC released statistics on its privacy and data security enforcement, finding that it has launched 75 general privacy lawsuits and 65 data security lawsuits since 2002.[67] The report announced that the agency had conducted enforcement actions in nine privacy cases and six data security cases that year. Those numbers are likely higher given the FTC does not pursue cases against every company it investigates (although every company investigated incurs compliance costs). Given expanded authority under the FTC act, we conservatively concluded that federal privacy legislation could result in 15 FTC investigations related to privacy each year (although this number could be significantly higher depending on funding and authority expansions).

Regarding state enforcement actions, state attorneys general vary widely in the number of consumer protection lawsuits they initiate. For example, while New York launched 103 investigations in 2015, California only initiated 23 in that time.[68] And in 2013, states and the District of Columbia averaged 15 consumer protection lawsuits each.[69] This number applies to all types of consumer protection statutes against entities in financial services, consumer services, insurance, health care, pharmaceuticals, etc. Given this number is spread across several consumer protection statutes, and the increasing prevalence of data privacy and security lawsuits since the time of these reports, we predict states (and the District of Columbia) will average approximately eight lawsuits related to privacy or data security each on an annual basis.[70] Given these assumptions, states could bring roughly an additional 400 lawsuits.

To ascertain how many of these federal and state cases are duplicative or frivolous, we used the number of dismissals of these cases as a metric. In 2015, approximately 50 percent of consumer protection claims were dismissed.[71] Therefore, roughly 200 state lawsuits and 10 federal lawsuits could be dismissed.

There are significant costs, such as lawyer and court fees, associated with defending lawsuits filed by regulators. To fight each such case, organizations must cover significant costs and fees—even when they are ultimately successful. To calculate them, we used the FTC's case against LabMD as a benchmark.[72] LabMD had claimed that the company—which was ultimately successful against the FTC's lawsuit, but went out of business due to the fees associated with that lawsuit—spent $1.8 million in attorneys' fees and other associated costs.[73] Using a discounted rate of $1 million per incident, duplicative and frivolous lawsuits could result in roughly $210 million in legal costs each year.

In addition, some privacy laws enable private right of action. These provisions enable class-action lawsuits for large incidents. It is likely federal privacy legislation that creates a private right of action for violations would result in an increase in lawsuits. To estimate this amount, we used the costs associated with class-action lawsuits. A 2018 survey of general counsel or senior legal officers at 395 Fortune 1000 and other large companies across a variety of industries found that in 2018, spending on class-action lawsuits rose to its highest recorded amount of $2.46 billion worldwide.[74] Companies that were surveyed also predicted data privacy and security class actions would increase in 2019.[75] A 2008 survey from Duke Law School found that the average outside litigation costs per respondent was $115 million, a figure that has only increased since that time.[76] We therefore conservatively predict class-action lawsuits will cost organizations roughly $50 million dollars each.

Given federal class actions for consumer protection statutes were six-times more likely to occur in federal than state courts in 2015—271 federal versus 107 state cases—federal legislation with a private right of action will only encourage these types of lawsuits.[77] Unfortunately, some of them will be duplicative or frivolous. For example, 54 percent of the securities class-action lawsuits filed in 2017 were dismissed.[78] In another 2013 study of 148 class actions, not a single case went to trial—as 25 percent were dismissed, 30 percent were voluntarily dismissed, settled, or remained pending four years after being filed.[79] We conservatively estimate that a federal private right of action could result in 100 lawsuits annually, of which 50 percent will be dismissed.[80] Given these parameters, private right of action could lead to fees of an additional $2.5 billion annually.

Figure 9: Costs associated with duplicative enforcement

Description	# of Requests	$ per Request	Cost
Federal Lawsuits	10	$1,000,000	$10 M
State Lawsuits	200	$1,000,000	$200 M
Class Action Lawsuits	50	$50,000,000	$2,500 M
Total			**$2,710 M**

Therefore, the cost of duplicative and frivolous enforcement resulting from regulators pursuing the same cases would be roughly $2.7 billion.

Lower Consumer Productivity

Privacy regulations usually create additional transparency requirements to help users better understand their rights and how their information is collected and used. While these components are intended, through increased transparency in business practices, to enable consumers to make more informed decisions about how they share their personal data, they also take time to review and respond to. This primarily occurs when privacy laws are drafted ways that lead to pop-up notices users must click through in order to access content.

For example, in 2009, the European Union (EU) modified its Directive on Privacy and Electronic Communications, also known as the e-Privacy Directive (ePD), to regulate browser cookies (a cookie is generally classified by its lifespan and the domain to which it belongs, and can either be a session cookie, which is erased after users close their browser, or a persistent cookie, which remains on the device for a predefined period of time).[81] The ePD creates rules for each of these cookies, requiring prior informed consent. As a result, most European website operators have added a banner or pop-up notification about each website's use of cookies. And after the passage of the GDPR, these pop-up notices have become even more common on websites.

The average productivity loss of U.S. consumers accessing online services would be roughly $1.9 billion.

We estimated the productivity cost of these types of polices based on the time it takes U.S. website users to read and click on notifications. To calculate for productivity, we first accounted for Internet users who were employed and those who were unemployed (either in the labor force but out of work, or not actively looking for work). Based on population and Internet usage data, we estimated that there are 180 million Internet users in the United States' active labor force.[82] There are an estimated 58 million retired or otherwise not employed U.S. adult Internet users.[83] We assumed the average adult Internet user visits 92 unique websites per month, which was based on a 2013 Nielsen report that reviewed the browsing behavior of U.S. Internet users.[84] While Internet usage has increased since 2013, we chose to keep this metric, as it had not been updated and provided a conservative base for our assumptions.[85]

To account for users visiting the same domain each month (and therefore not needing to re-read and re-click the cookie notice), we discounted this number by 50 percent, assuming it takes U.S. Internet users at least 2 seconds to notice, read, and click on the cookie notification. This benchmark is conservative because some users may take longer to read the notification if it appears in a text pop-up, while others may ignore the message altogether. Based on these estimates, a pop-up notice policy would result in 9.2 million wasted hours each month in the active labor market, and 3.0 million wasted hours in the inactive labor market.

We calculated the productivity loss based on the number of wasted hours and the median gross hourly earnings for an individual living the United States. Based on the Bureau of Labor Statistics, the median gross hourly earnings is $18.58 per hour, which we rounded to $18.60 per hour.[86] We conservatively concluded that working adults spend half their time on the Internet for work and half for leisure. To calculate the productivity costs for leisure, we used a discounted hourly wage—a type of discount that has been used to measure economic costs of personal time,

such as time spent in traffic. For example, personal travel time is usually estimated between 25 and 50 percent of prevailing wages, based on a variety of factors such as distance, traveler, and road conditions.[87] Using this metric as a guide, we selected a 50 percent discount for this hourly wage to account for leisure. We then applied this discount to both the portion of time wasted by workers (half, as previously mentioned), and to all of the time wasted by nonworkers to account for leisure. Using these estimates, we calculated the average productivity cost in the active labor market to be $128 million per month, and $28 million per month in the inactive labor market.

Based on this data, the projected productivity cost of a U.S. pop-up consent notice policy for U.S. citizens each year would be $1.9 billion.

Figure 10: Productivity costs associated with pop-up notifications

Description	# of Hours	$ per Hour	Cost
Active labor market	110 M	$18.60	$1,540 M
Inactive labor market	36 M	$18.60	$331 M
Total			**$1,870 M**

MARKET INEFFICIENCIES

In addition to the direct costs of data protection regulation, there are indirect costs that adversely impact how organizations can innovate. Many of these types of privacy rules center around constructing barriers to firms attempting to collect or use information. If the United States were to enact overly restrictive privacy legislation, **it could generate roughly $104 billion in market inefficiencies,** which would be borne out in increased costs, decreased productivity (for both organizations and consumers), and decreased innovation**.** Similar to compliance costs, these inefficiencies would increase if the federal data protection law did not preempt state legislation. Exact estimates are difficult to predict and may change depending on the number of state regimes and the provisions included therein.

Certainly, there are numerous ways such legislation can generate inefficiencies, including increased market uncertainty, productivity losses, reduced ability to innovate, and more. To avoid "boiling the ocean," we selected two types of inefficiencies associated with privacy legislation: less access to data and lower ad effectiveness—although this list is certainly not exhaustive.

Reduced Access to Data

Various data privacy rules—such as requirements for express consent, data minimization, or purpose specification—can reduce access to data, limit data sharing, and constrain its use, thereby limiting innovation.[88]

For example, opt-in consent requirements may require organizations to obtain affirmative consent from individuals before using their information for all but the most narrow range of purposes (e.g., delivering a package).[89] Unfortunately, opt-in requirements frame consumer choices in a way that leads to suboptimal data sharing because most users select the default option of not giving consent—for a number of irrational reasons.[90] As a result, fewer users share their data, resulting in less data available and reduced innovation. Opt-in requirements would also raise

costs and reduce revenues, which organizations would have to pass on to consumers in the form of higher prices or lower-quality services.[91]

In addition, data minimization, which requires an organization to collect no more data than is necessary to meet specific needs (e.g., processing a payment), is frequently proposed for data privacy legislation. Unfortunately, this restriction negatively impacts organizations that do not know which data will be most valuable when initially deciding what data to collect. Data minimization can also hurt existing businesses by limiting their ability to conduct post hoc analyses to develop new types of products and services based on what they learn from the data—even if they use this data in a way that protects individual privacy.

Purpose specification requires organizations to disclose to users the purposes for which they are collecting information and then not use this collected data for any other reasons. This requirement limits organizations from reusing data for new purposes, which limits innovation. Purpose specification requirements also limit organizations that may already be collecting useful data from extracting value from that information, such as by applying data analytics, thereby also slowing the pace of innovation.

Restricting organizations from collecting, sharing, and using data limits their ability to improve productivity, as doing so prevents them from automating processes, optimizing business decisions, and discovering new customers. A retailer, for example, may not be able to successfully deploy an automated system for screening job applicants, discover new product ideas based on social media trends, or prioritize outreach to prospective customers based on their interests. Making sense of the vast amounts of data collected about people and the world around them is also necessary to address major social challenges, including improving health care, education, public safety, transportation, energy, and the environment. Restrictions on data impede these important missions.

The GDPR imposes opt-in consent, data minimization, and purpose specification requirements. Moreover, many different U.S. legislators have proposed bills with these components. For example, Sen. Ed Markey's (D-MA) bill, the Privacy Bill of Rights Act, would create data minimization requirements.[92]

If federal privacy legislation substantially limited organizations from collecting, using, and sharing data, it could cost $71 billion annually in lost value across the U.S. economy.

If policymakers restrict how firms collect, use, and share data, it would limit how organizations generate value from data, resulting in data functions of the economy growing more slowly than they would have otherwise. McKinsey Global Institute has documented several "game changing" areas where better access and processing of data could boost the U.S. economy by billions of dollars of gross domestic product and create a boon in jobs, much of which would come from data analytics in traditional industries.[93]

To quantify how data protection rules can result in a loss of value produced by sharing data, we used metrics from a McKinsey report that predicted the annual value that increased data sharing could bring to the economy.[94] The 2013 report estimated that if organizations in both the public and private sector shared more data, this data could generate roughly $3.2 trillion globally in additional value each year in seven industries, of which $1.3 trillion would benefit the United States.[95] This overall estimate of $1.3 trillion each year breaks down as follows for seven U.S.

industries: $360 billion in the education sector, $290 billion in the transportation sector, $210 billion for consumer products, $140 billion for electricity, $100 billion for oil and gas, $100 billion for health care, and $80 billion for consumer finance. In addition, we assume another $100 billion in potential value from increased data sharing for the remaining sectors, such as retail, real estate, and security.

Restricting data sharing through federal data privacy legislation could cause these sectors to lose 5 percent of the value of data sharing described in McKinsey's report.[96] This estimate is conservative given health care, education, and finance each rely heavily on personal data as part of their business practices. Therefore, this number is possibly much higher. Certainly, the previously detailed seven sectors would be impacted in different ways depending on how much they rely on user information. For example, oil and gas businesses may not be as impacted as consumer finance industries that rely more heavily on user data to innovate. The loss of 5 percent is therefore averaged across all seven sectors.

If federal data privacy legislation substantially limited organizations from collecting, using, and sharing data, the United States would lose $71 billion in value across the seven sectors.

Figure 11: Estimated inefficiencies associated with reduced access to data across these sectors

Sector	Cost
Education	$18,000 M
Transportation	$14,500 M
Consumer Products	$10,500 M
Electricity	$7,000 M
Oil and Gas	$7,000 M
Healthcare	$5,000 M
Consumer Finance	$4,000 M
Other	$5,000 M
Total	**$71,000 M**

Lower Ad Effectiveness

Targeted advertising is beneficial to consumers and businesses alike, allowing firms to be more efficient with their resources while increasing sales—all while reducing the number of advertisements.[97] Consumers benefit by gaining more utility from relevant ads, such as by learning about products that are similar to past purchases and getting access to free or low cost services.[98] In addition, overall economic welfare increases as organizations become more efficient and are able to reduce prices while improving their products and services. In 2010, McKinsey Institute and IAB Europe estimated that the consumer surplus—the difference between what consumers are willing to pay for a product or service and what they actually do pay—from ad-supported Internet sites (after discounting the "costs" of privacy and ads) was $44 billion per year in the United States.[99] As such, any data privacy rules that unduly limit targeted advertising would reduce both producer and consumer welfare.[100]

Reducing the effectiveness of advertising would have deleterious effects throughout the digital ecosystem. For example, regulations that shift online services from an opt-out privacy system, in which consumers can choose to not have their data used by a company, to an opt-in privacy system, in which organizations can only use data after obtaining affirmative consent from users, will adversely affect advertising-based business models.[101] Indeed, a 2011 study found that EU privacy regulation requiring an opt-in system has decreased the effectiveness of online advertising, thereby reducing the revenue of websites that rely on ad-based business models.[102] This approach was further adopted for all personal data usage in the GDPR, and several U.S. policymakers have suggested adopting it, in part, in the United States.[103]

If federal privacy legislation drastically limited the effectiveness of advertising—such as by creating a do-not-track mandate or affirmative consent requirements—it could result in an annual loss of roughly $33 billion in economic value in the U.S. digital economy.

A report from 2014 concluded that firms enabling the use of personal data for marketing contributed $202 billion in value to the U.S. economy.[104] These benefits included more efficient marketing strategies, greater marketing insights, and lower barriers to entry for marketing among smaller firms challenging incumbents. More than half of this amount, which accounted for roughly $102 billion of revenue and almost 150,000 jobs, depended directly or indirectly on third-party data.[105] To estimate the impact on the reduced effectiveness of advertising of any proposed rule, we assumed restrictions would impact all advertising, and have a greater impact on third-party advertising. We also assumed the ratio of first-party advertising to third-party advertising remained the same from 2014 to 2018.[106] Given advertising revenues increased to roughly $107.5 billion in 2018, if each type of advertising had commanded roughly half the revenue, both first-party and third-party advertising would have been responsible for roughly $53.8 billion.

Next, we tried to establish the extent to which rigorous privacy regulations would impact these revenues. According to one study, restrictive European regulation that included an affirmative consent privacy policy resulted in an average reduction in the effectiveness of online ads by approximately 65 percent.[107] To keep our estimates conservative, we will only assume a 5-percent drop in effectiveness in first-party advertising and a 10-percent drop in effectiveness of third-party advertising. We differentiated between these two types of ads because a reduction of effectiveness in advertising would impact third-party ads more than their first-party counterparts. Given these estimates, we can reasonable conclude that burdensome rules could result in a decline of 8 percent, or roughly $8 billion, in advertising revenues.

To calculate how the decreased effectiveness of online advertising might impact the value of the digital economy, we compared the relative digital ad revenues between 2014 and 2018. In 2014, according to the Interactive Advertising Bureau (which tracks revenues each year), the Internet advertising revenues in the United States totaled $49.5 billion.[108] By contrast, that number had increased to $108 billion in 2018.[109] Given $49.5 billion in revenues supported $202 billion in value in the digital economy in 2014, we can assume $108 billion in revenues supported roughly $439 billion in 2018. Therefore, an 8-percent decrease in online ad revenues in 2018 would have led to a loss of roughly $33 billion in economic value from the digital economy.

THE COSTS OF TARGETED REGULATION

Rather than pass unnecessarily stringent data privacy legislation at great expense to the U.S. economy, Congress can create a more targeted set of rules that still protect consumers but do so at a much more reasonable cost. This optimal solution would maximize consumer welfare by enhancing consumer privacy, but minimize the law's impact on prices and access to free services. If Congress enacts a more focused national data privacy law, **we predict it will cost approximately $6.5 billion per year**—around 95 percent less than it would cost to pursue a European-style data protection law.

ITIF outlined in a previous report several specific recommendations for what Congress should include in a federal privacy law.[110] Our estimate is based on several key components we believe are necessary in federal privacy legislation, including creating requirements for privacy audits, improving government enforcement, and establishing a set of user rights.

First, federal data privacy legislation should include an oversight component, including through privacy compliance audits and the processing of complaints by federal regulators. We did not estimate costs for federal or state agencies in this report. That said, privacy audit requirements could cost U.S. organizations $444 million each year based on the estimates above.

Second, federal data privacy legislation should improve enforcement without creating an overly duplicative or frivolous regime. To that end, Congress should not allow a private right of action, and instead rely on federal and state regulators to hold organizations accountable. This would minimize the majority of the unnecessary spending on excessive enforcement actions, although there would still be roughly $212 million each year in duplicative enforcement expenses from having multiple regulators.

Third, federal privacy legislation should give consumers more control over their data, including the ability to access, port, delete, and rectify their data, while also minimizing compliance costs in a few important ways. For example, Congress can allow organizations to recoup some costs associated with fulfilling requests for data access and portability—especially those associated with lengthy or difficult requests. Enabling organizations to do so would reduce the number of excessive and duplicative requests organizations might face, and encourage individuals to only request data that is of value. Moreover, Congress has the ability to only require certain organizations, such as those processing sensitive data in certain industries, to provide these types of user control, rather than applying it across the board to all organizations processing personal data.[111] By limiting when these requirements apply, we believe Congress can reduce costs for data access, portability, deletion, and rectification to roughly 25 percent of our original estimates. Importantly, organizations would still incur costs associated with developing and maintaining data infrastructure to facilitate requests, but receive significantly fewer requests overall across each type. Costs associated with facilitating user requests therefore include $4.8 billion for data infrastructure, $212 million for access, $127 million for data portability, $193 million for deletion, and $48 million for rectification. These estimates would shift depending on how lawmakers elected to constrain costs associated with any individual request.

Importantly, these estimates do not consider the costs associated with different jurisdictions creating conflicting standards for data privacy. If federal privacy legislation fails to preempt states from creating their own different sets of data privacy laws, costs could increase significantly.

Figure 12: Costs associated with targeted regulation

Description	Cost
Privacy Audits	$440 M
Enforcement	$210 M
Data Infrastructure	$5,380 M
Data Access	$90 M
Data Portability	$130 M
Data Deletion	$200 M
Data Rectification	$50 M
Total Cost	**$6,500 M**

CONCLUSION

Before policymakers in the United States create federal privacy rules, or continue to allow states to create a patchwork of different regulations, they need to have an understanding of the costs involved in such rules. Indeed, overly restrictive rules for the digital economy reduce innovation in ways that harm both businesses and consumers. By raising compliance costs, increasing legal risks, and reducing the effectiveness of online business models, poorly drafted rules lead to a reduction in the supply of, and demand for, digital services.

Therefore, it is absolutely necessary to create federal privacy rules to ensure broad and equal protections for users while reducing uncertainty and compliance costs for covered organizations. But such a task should not be undertaken lightly. To that end, these back-of-the-envelope estimates may help some policymakers understand which provisions in privacy rules may be the costliest—and rightfully should receive more skepticism and attention to detail.

ABOUT THE AUTHORS

Alan McQuinn is a senior policy analyst at the Information Technology and Innovation Foundation. He writes and speaks on a variety of issues related to information technology and Internet policy, such as cybersecurity, privacy, blockchain, fintech, e-government, Internet governance, intellectual property, and aerospace. He was previously a telecommunications fellow for Representative Anna Eshoo (D-CA). McQuinn graduated from the University of Texas at Austin with a B.S. in public relations and political communications and a minor in Mandarin Chinese.

Daniel Castro is vice president of ITIF and director of ITIF's Center for Data Innovation. His research interests include health IT, data privacy, e-commerce, e-government, electronic voting, information security, and accessibility. Before joining ITIF, Castro worked as an IT analyst at the Government Accountability Office, where he audited IT security and management controls at various government agencies. He has a B.S. in foreign service from Georgetown University and an M.S. in information security technology and management from Carnegie Mellon University.

ABOUT ITIF

The Information Technology and Innovation Foundation (ITIF) is a nonprofit, nonpartisan research and educational institute focusing on the intersection of technological innovation and public policy. Recognized as the world's leading science and technology think tank, 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. Alan McQuinn and Daniel Castro, "Why Stronger Privacy Regulations Do Not Spur Increased Internet Use" (Information Technology and Innovation Foundation, July 2018), http://www2.itif.org/2018-trust-privacy.pdf.
2. U.S. Bureau of Labor Statistics, Average Expenditure (Size of consumer unit; accessed July 23, 2019), https://www.bls.gov/cex/tables.htm#annual.
3. Daniel Castro and Travis Korte, "Data Innovation 101" (Center for Data Innovation, November 2013), https://www.datainnovation.org/2013/11/data-innovation-101/.
4. Nick Wallace et al., "How Canada, the EU, and the U.S. Can Work Together to Promote ICT Development and Use" (Information Technology and Innovation Foundation, June 2018), http://www2.itif.org/2018-canada-eu-us-ict-development.pdf.
5. Alan McQuinn and Daniel Castro, "A Grand Bargain on Data Privacy Legislation for America" (Information Technology and Innovation Foundation, January 2019), http://www2.itif.org/2019-grand-bargain-privacy.pdf.
6. "Consumer Data Privacy Legislation," National Conference of State Legislatures, June 17, 2019, accessed July 24, 2019, http://www.ncsl.org/research/telecommunications-and-information-technology/consumer-data-privacy.aspx.
7. Cameron Kerry, "Breaking Down Proposals for Privacy Legislation: How do they Regulate?" (Brooklings, March 8, 2019), accessed July 23, 2019, https://www.brookings.edu/research/breaking-down-proposals-for-privacy-legislation-how-do-they-regulate/.
8. McQuinn and Castro, "Why Stronger Privacy Regulations Do Not Spur Increased Internet Use."
9. Marc Vartabedian, "California Passes Sweeping Data-Privacy Bill," *Wall Street Journal*, June 28, 2018, accessed July 23, 2019, https://www.wsj.com/articles/california-rushes-to-tighten-data-privacy-restrictions-1530190800.
10. California Consumer Privacy Act, California Civil Code § 1798.125.
11. "Global 500 Companies to Spend $7.8B on GDPR Compliance" (International Association of Privacy Professionals, November 20, 2017), accessed July 23, 2019, https://iapp.org/news/a/survey-fortune-500-companies-to-spend-7-8b-on-gdpr-compliance/.
12. PwC, "GDPR Compliance Top Data Protection Priority for 92% of US Organizations in 2017, According to PwC Survey," news release, January 23, 2017, accessed July 23, 2019, https://www.pwc.com/us/en/press-releases/2017/pwc-gdprcompliance-press-release.html.
13. U.S. Census Bureau, Country Business Patterns, (enterprise employment size, by NAICS and number of establishments, accessed June 10, 2019), https://www.census.gov/data/tables/2016/econ/susb/2016-susb-annual.html.
14. "HIPAA Cost Considerations" Principle Logic, LLC, October 11, 2003, accessed July 23, 2019, https://www.principlelogic.com/wp-content/uploads/2018/06/HIPAAPSC_Ch3.pdf; Department of Health and Human Services, "Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules," Government Publishing Office, January 25, 2013, accessed July 23, 2019, https://www.govinfo.gov/content/pkg/FR-2013-01-25/pdf/2013-01073.pdf; Indeed, HHS estimated the HITECH Act, which updated HIPAA in 2013, would add an additional $114 million to $225 million in compliance costs for the first year of implementation, and $14.5 million annual costs thereafter, depending on the size of the covered entity.
15. "Amendment to the Annual Privacy Notice Requirement Under the Gramm-Leach-Bliley Act (Regulation P)," Consumer Financial Protection Bureau, August 17, 2018, accessed July 30, 2109,

https://www.federalregister.gov/documents/2018/08/17/2018-17572/amendment-to-the-annual-privacy-notice-requirement-under-the-gramm-leach-bliley-act-regulation-p.

16. McQuinn and Castro, "Why Stronger Privacy Regulations Do Not Spur Increased Internet Use."
17. It is likely that many firms, especially those already subject to sector-specific regimes, are actively implementing these provisions. Therefore, estimates may be higher than expected. We tried to address this by making our estimates sufficiently conservative.
18. "Consumer Data Protection Act Discussion Draft," Office of Sen. Ron Wyden, accessed July 23, 2019, https://www.wyden.senate.gov/imo/media/doc/Wyden%20Privacy%20Bill%20Discussion%20Draft%20Nov%201.pdf; Balancing the Rights of Web Surfers Equally and Responsibly Act, H.R. 2520 (2017), 115th Cong. (2017).
19. Riley Panko, "Why Small Businesses Lack Accounting Resources in 2018" Clutch, October 1, 2018, accessed July 23, 2019, https://clutch.co/accounting/resources/why-small-businesses-lack-accounting-resources-2018.
20. "2018 CPAFMA IT Benchmark Survey Findings" (CPA Firm Management Association, January 25, 2018), accessed July 23, 2019, https://cpafma.org/articles/2018-cpafma-benchmark-survey-findings.
21. Because exact estimates are difficult to obtain elsewhere, these estimates are our best-guess.
22. "ICB Survey Results" (The Institute of Certified Bookkeepers, 2017), accessed July 23, 2019, https://www.icb.org.au/About-Bookkeepers/ICB-Annual-Survey-2017.
23. U.S. Census Bureau, Country Business Patterns, (enterprise employment size, by NAICS and number of establishments; accessed June 10, 2019), https://www.census.gov/data/tables/2016/econ/susb/2016-susb-annual.html.
24. Brice McKeever, "The Nonprofit Sector in Brief" (National Center for Charitable Statistics, January 3, 2019), accessed July 23, 2019, https://nccs.urban.org/project/nonprofit-sector-brief.
25. "Privacy Officer Salaries in United States," Glassdoor, updated July 12, 2019, accessed July 23, 2019, https://www.glassdoor.com/Salaries/us-privacy-officer-salary-SRCH_IL.0,2_IN1_KO3,18.htm.
26. "Indirect Rates for Government Contractors" (Arrowhead Solutions, LLC, 2015), accessed September 23, 2019, https://www.arrowheadsolutionsllc.com/files/Indirect%20Rates%20for%20Government%20Contractors%20Overview.pdf.
27. "2017 Government Contractor Survey" (GrantThorton and Professional Services Council, Spring 2018), accessed July 23, 2019, https://www.grantthornton.com/-/media/content-page-files/public-sector/pdfs/surveys/2018/2017-government-contractor-survey.
28. "Processor," Regulation (EU) 2016/679 (General Data Protection Directive), Art. 28, https://gdpr-info.eu/art-28- gdpr/.
29. John Kennedy, "Majority of Organizations Expect a GDPR Audit in the Next 18 Months," *Silicon Republic*, December 6, 2017, accessed July 23, 2019, https://www.siliconrepublic.com/enterprise/gdpr-audit.
30. European Data Protection Board, "First Swedish GDPR Audit Completed," news release, October 23, 2018, https://edpb.europa.eu/news/national-news/2018/first-swedish-gdpr-audit-completed_en.
31. "Audit Protocol – Update July 2018," U.S. Department of Health and Human Services, July 2018, accessed July 23, 2019, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html.
32. Data Care Act of 2018, S. 3744 (2018), 115th Cong. (2018); Algorithmic Accountability Act of 2019, S.1108 (2019), 116th Cong. (2019).

33. Because exact estimates are difficult to obtain elsewhere, these estimates are best-guess. The amount is likely higher because many firms will do a self-audit to ensure they could do a real audit.
34. 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/.
35. 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/.
36. Ibid.
37. "2017 State of Authentication Report" (FIDO Alliance, October 2017), accessed July 23, 2019, https://fidoalliance.org/wp-content/uploads/The-State-of-Authentication-Report.pdf.
38. "Four barriers to Adopting Strong Authentication" (Nok Nok Labs, July 2014), accessed July 24, 2019, https://www.noknok.com/wp-content/uploads/2017/10/4barrierswhitepaper_0.pdf.
39. Joshua New, "AI Needs Better Data, Not Just More Data," Center for Data Innovation, March 20, 2019, accessed July 23, 2019, https://www.datainnovation.org/2019/03/ai-needs-better-data-not-just-more-data/.
40. Tadhg Nagle, Thomas Redman, and David Sammon, "Only 3 Percent of Companies' Data Meets Basic Quality Standards," *Harvard Business Review*, September 11, 2017, accessed July 23, 2019, https://hbr.org/2017/09/only-3-of-companies-data-meets-basic-quality-standards.
41. Armand Ruiz, "The 80/20 Data Science Dilemma," *InfoWorld*, September 26, 2017, accessed July 23, 2019, https://www.infoworld.com/article/3228245/the-80-20-data-science-dilemma.html.
42. "Data Analyst Salaries," Glassdoor, updated July 23, 2019, accessed July 23, 2019, https://www.glassdoor.com/Salaries/data-analyst-salary-SRCH_KO0,12.htm.
43. McQuinn and Castro, "A Grand Bargain on Data Privacy Legislation for America."
44. "Subject Access Requests to GP Practices Increase by a Third Since GDPR Legislation Came In" (British Medical Association, December 2018), accessed July 23,2019, https://www.bma.org.uk/news/media-centre/press-releases/2018/december/subject-access-requests-to-gp-practices-increase-by-a-third-since-gdpr-legislation-came-in.
45. "Privacy," RBS, March 2017, accessed July 23, 2019, https://www.rbs.com/rbs/sustainability/customer-focused/privacy.html.
46. "Ship Your Enemies GDPR," ShipYourEnemiesGDPR, accessed July 23, 2019, https://shipyourenemiesgdpr.com/.
47. Tom Le Bras, "Online Overload – It's Worse Than You Thought," *Dashlane blog*, July 21, 2015, accessed July 23, 2019, https://blog.dashlane.com/infographic-online-overload-its-worse-than-you-thought/. This estimate accounts for the active and inactive labor market in the United States. We multiplied this number of people by the Internet penetration in the United States (i.e., 90 percent).
48. Because exact estimates are difficult to obtain elsewhere, these estimates are our best-guess.
49. Leandra English and Stephen Brobeck, "Survey Shows An Increasing Number of Consumers Have Obtained Their Credit Scores and Know Much More About Credit Scores," *Consumer Federation of America*, press release, June 18, 2018, accessed July 23, 2019, https://consumerfed.org/press_release/survey-shows-an-increasing-number-of-consumers-have-obtained-their-credit-scores-and-know-much-more-about-credit-scores/.
50. "Identity Cloud Pricing," Okta, accessed July 23, 2019, https://www.okta.com/pricing/; "Verify Your Customers in Seconds," Yoti, accessed July 23, 2019, https://www.yoti.com/business/pricing/.
51. "Business Credit Report Survey," The Kaplan Group and TKG, February 2015, accessed July 23, 2019, https://www.kaplancollectionagency.com/wp-content/uploads/2012/07/Business-Credit-Report-Survey-Version-1.02.pdf.

52. Ohio Credit Union League, "Request for Information Regarding Consumers' Experience with Free Access to Credit Scores Docket," letter to Consumer Financial Protection Bureau, No.: CFPB-2017-0037, February 12, 2018, accessed July 24, 2019.
53. Trevor Hughes and Angela Saverice-Rohan, "IAPP-EY Annual Privacy Governance Report 2017" (IAPP, EY, 2017), accessed July 23, 2019, https://iapp.org/media/pdf/resource_center/IAPP-EY-Governance-Report-2017.pdf.
54. Daniel Castro and Michael Steinberg, "Blocked: Why some Companies Restrict Data to Reduce Competition and How Open APIs Can Help" (Center for Data innovation, November 6, 2017), http://www2.datainnovation.org/2017-open-apis.pdf.
55. Because exact estimates are difficult to obtain elsewhere, these estimates are our best-guess.
56. Leandra English and Stephen Brobeck, "Survey Shows An Increasing Number of Consumers Have Obtained Their Credit Scores and Know Much More About Credit Scores," *Consumer Federation of America*, press release, June 18, 2018, accessed July 23, 2019, https://consumerfed.org/press_release/survey-shows-an-increasing-number-of-consumers-have-obtained-their-credit-scores-and-know-much-more-about-credit-scores/.
57. "Data Sharing and Open Data For Banks" (Open Data Institute and Fingleton Associates, September 2014), accessed July 24, 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/382273/141202_API_Report_FINAL.PDF .
58. Regulation (EU) 2016/679 (General Data Protection Directive), OJ L 119, March 05, 2016, Articles 1-99, http://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN.
59. California Consumer Privacy Act, California Civil Code § 1798.125
60. Ryan Law, "Churn Rate: How High is Too High? A Meta-Analysis of Churn Studies," *Bloom*, May 28, 2019, accessed July 23, 2019, https://www.cobloom.com/blog/churn-rate-how-high-is-too-high.
61. McQuinn and Castro, "A Grand Bargain on Data Privacy Legislation for America."
62. Consumer Federation of America, "Survey Shows An Increasing Number of Consumers Have Obtained Their Credit Scores and Know Much More About Credit Scores," press release, June 18, 2018, accessed July 24, 2019, https://consumerfed.org/press_release/survey-shows-an-increasing-number-of-consumers-have-obtained-their-credit-scores-and-know-much-more-about-credit-scores/; "Report to Congress Under Sector 319 of the Fair and Accurate Credit Transactions Act of 2003," (U.S. Federal Trade Commission, December 2012), accessed July 24, 2019, https://www.ftc.gov/sites/default/files/documents/reports/section-319-fair-and-accurate-credit-transactions-act-2003-fifth-interim-federal-trade-commission/130211factareport.pdf. In 2018, 38 percent of U.S. consumers had obtained their credit report (the full report rather than simply the score) in the previous year. Of these, the FTC estimated 21 percent of consumers had requested a modification for at least one of their credit reports in 2012.
63. Google, Transparency Report (Search Removals Under European Privacy Law, accessed July 2019), https://transparencyreport.google.com/eu-privacy/overview?hl=en. We looked at the number of RTBF requests in 2018 for the United Kingdom, France, Germany, and Finland, and compared those rates with the ITU estimates for fixed broadband subscribers in those countries in 2017. While rates varied between 0.06% and 0.1%, we chose to use the 0.1%. This is because few accounts make up for the bulk of requests, and access requests are more likely than delisting requests.
64. The Federal Trade Commission Act, 15 U.S.C. § 41 (1914).
65. Ally Marotti, "Shutterfly Lawsuit Tags Illinois As Battleground in Facial Recognition Fight," *Chicago Tribune*, September 21, 2017, accessed July 23, 2019, https://www.chicagotribune.com/business/ct-biz-biometricsshutterfly-lawsuit-20170920-story.html.
66. Regulation (EU) 2016/679 (General Data Protection Directive).

67. "Privacy & Data Security Update: 2018" (U.S. Federal Trade Commission, March 2019), accessed July 23, 2019, https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2018/2018-privacy-data-security-report-508.pdf.
68. James Cooper and Matthew Sibery, "State Consumer Protection Act Litigation: Update on Trends" (George Mascon University Law & Economics Center, June 2016), accessed July 23, 2019, http://www.civiljusticenj.org/wp-content/uploads/2018/02/16June_StateConsumerProtectionActLitigation.pdf.
69. Ibid.
70. Ray Pompon, "Breach Costs Are Rising with the Prevalence of Lawsuits," Application Threat Intelligence, May 2, 2018, accessed July 23, 2019, https://www.f5.com/labs/articles/cisotociso/breach-costs-are-rising-with-the-prevalence-of-lawsuits.
71. Cooper and Sibery, "State Consumer Protection Act Litigation: Update on Trends. This differs slightly between states and federal courts.
72. LABMD, Inc v. Federal Trade Commission, On Petition for review of an Order of the Federal Trade Commission (FTC Docket No, 9357), https://www.ftc.gov/system/files/documents/cases/labmd_ca11_ftc_opposition_to_fee_request_2018-1119.pdf.
73. Ibid; Dune Lawrence, "A Leak Wounded This Company. Fighting the Feds Finished It Off," *Bloomberg*, April 25, 2016, accessed July 23, 2019, https://www.bloomberg.com/features/2016-labmd-ftc-tiversa/.
74. "2019 Carlton Fields Class Action Survey," (Carlton Fields, 2019), accessed July 23, 2019, https://gallery.mailchimp.com/0c82d1e732eec64ff4cb3d4b7/files/d46d1d29-390d-48ec-ac98-50c7e8600edc/2019_Class_Action_Survey.pdf.
75. Ibid.
76. "Litigation Cost Survey of Major Companies" (Lawyers for Criminal Justice, Civil Justice Reform Group, U.S. Chamber Institute for Legal Reform, May 2010), accessed July 23, 2019, https://www.uscourts.gov/sites/default/files/litigation_cost_survey_of_major_companies_0.pdf.
77. Cooper and Sibery, "State Consumer Protection Act Litigation: Update on Trends"
78. Baker McKenzie, "Securities Law Class Actions are Mushrooming, But More Cases are Being Dismissed and the Survivors are Settling for Less," *Lexology*, accessed July 23, 2019, https://www.lexology.com/library/detail.aspx?g=0f4c442b-750b-4c48-baea-71566dc535b5.
79. "Do Class Actions Benefit Class members? An Empirical Analysis of Blass Actions" (Mayer Brown LLP, 2013), accessed July 23, 2019, https://www.instituteforlegalreform.com/uploads/sites/1/Class_Action_Study.pdf.
80. Because exact estimates for the number of lawsuits are difficult to obtain elsewhere, these estimates are best-guess. We tried to keep the estimates conservative to account for this ambiguity.
81. Daniel Castro, "Federal Government Policy on the Use of Persistent Internet Cookies: Time for Change or More of the Same?" The Information Technology and Innovation Foundation, May 2009, http://www.itif.org/files/2009-FederalCookies.pdf.
82. Pew Research Center, Internet Use Over Time (U.S. Adults Who Use the Internet; accessed July 23, 2019), https://www.pewinternet.org/fact-sheet/internet-broadband/; U.S. Census Bureau, Census Bureau Projects U.S. and World Populations on New Year's Day (U.S. Population on January 1, 2019; accessed July 23, 2019), https://www.census.gov/newsroom/press-releases/2019/new-years-population.html; U.S. Bureau of Labor Statistics, The U.S. Labor Force Participation Rate – June 2019 (Labor Force Participation Rate; accessed July 23, 2019), https://www.bls.gov/news.release/pdf/empsit.pdf. Pew data shows Internet penetration is 90 percent.

Further, the active labor market is roughly 200 million as of April 2019, according to active labor force statistics from BLS and Census protections in 2019.

83. Given the United State' total population is estimated to be 327 million, and the active labor market is 200 million, we found the inactive market to be roughly 127 million. We then discounted to account for those aged 0–14-years-olds (19.1 percent). This gave an estimate of the number of U.S. citizens who were either retired or inactive with no kids to be 65 million. Given Pew data reported 90 percent of U.S. citizens use the Internet, we estimate the United States has roughly 58 million people in its inactive labor force.
84. "March 2013: Top Education and Career Sites and U.S. Web Brands," Nielsen, May 10, 2013, http://www.nielsen.com/us/en/insights/news/2013/march-2013--top-education---career-sites-and-u-sweb-brands.html.
85. Pew Research Center, Internet Use Over Time (U.S. Adults Who Use the Internet; accessed July 23, 2019), https://www.pewinternet.org/fact-sheet/internet-broadband/.
86. U.S. Bureau of Labor Statistics, May 2018 National Occupational Employment and Wage Estimates United States (Median Hourly Wage; accessed July 23, 2019), https://www.bls.gov/oes/current/oes_nat.htm#00-0000.
87. "Transportation Cost and Benefit Analysis II – Travel Time Costs," Victoria Transport Policy Institute, August 28, 2013, accessed July 23, 2019, http://www.vtpi.org/tca/tca0502.pdf.
88. Alan McQuinn and Daniel Castro, "A Grand Bargain on Data Privacy Legislation for America" (Information Technology and Innovation Foundation, January 2019), http://www2.itif.org/2019-grand-bargain-privacy.pdf.
89. McQuinn and Castro, "A Grand Bargain on Data Privacy Legislation for America."
90. Alan McQuinn, "The Economics of 'Opt-Out' Versus 'Opt-In' Privacy Rules," Information Technology and Innovation Foundation, October 6, 2017, accessed July 10, 2019, https://itif.org/publications/2017/10/06/economics-opt-out-versus-opt-in-privacy-rules.
91. McQuinn and Castro, "Why Stronger Privacy Regulations Do Not Spur Increased Internet Use."
92. Privacy Bill of Rights Act, S. 1214 (2019), 116th Cong. (2019).
93. Susan Lund et al., "Game Changers: Five Opportunities For U.S. Growth and Renewal" (McKinsey Global Institute, July 2013), accessed July 22, 2019, https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Americas/US%20game%20changers/MGI_Game_changers_US_growth_and_renewal_Full_report.ashx.
94. James Manyika et. al., "Open Data: Unlocking Innovation and Performance with Liquid Information" (McKinsey Global Institute, October 2013), accessed July 22, 2019, https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/open-data-unlocking-innovation-and-performance-with-liquid-information.
95. James Manyika et al., "Open Data: Unlocking Innovation and Performance with Liquid Information" (McKinsey Global Institute, October 2013), accessed July 22, 2019, https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/open-data-unlocking-innovation-and-performance-with-liquid-information.
96. Because exact estimates are difficult to obtain elsewhere, these estimates are our best-guess.
97. Thomas Lenard and Paul Rubin, "In Defense of Data: Information and the Costs of Privacy" (Technology Policy Institute, May 2009), accessed July 23, 2019, https://techpolicyinstitute.org/wpcontent/uploads/2009/05/in-defense-of-data-information-2007385.pdf.
98. Ibid.

99. "Consumers Driving the Digital Uptake" (IAB Europe and McKinsey Global Institute, September 2010), accessed July 23, 2019, https://www.youronlinechoices.com/white_paper_consumers_driving_the_digital_uptake.pdf

100. Hal Varian, "Economic Aspects of Personal Privacy," Privacy and Self-regulation in the Information Age (1996); Thomas Lenard and Paul Rubin, "In Defense of Data: Information and the Costs of Privacy," (Technology Policy Institute, May 2009), accessed June 10, 2019, https://techpolicyinstitute.org/wpcontent/uploads/2009/05/in-defense-of-data-information-2007385.pdf.

101. Goldfarb and Tucker, "Privacy Regulation and Online Advertising."

102. Avi Goldfarb and Catherine Tucker, "Privacy and Innovation" Innovation Policy and the Economy, University of Chicago Press, vol. 12(1), 2011, accessed on National Bureau of Economic Research, accessed July 24, 2019, http://www.nber.org/papers/w17124; Goldfarb and Tucker, "Privacy Regulation and Online Advertising."

103. Regulation (EU) 2016/679 (General Data Protection Directive); The Customer Online Notification for Stopping Edge-provider Network Transgressions Act, S. 2639 (2018), 115th Cong. (2018).

104. John Deighton and Peter Johnson, "The Value of Data," *Direct Marketing Association and the Data-Driven marketing Institute,* December 2015, accessed July 23, 2019, https://thedma.org/wp-content/uploads/Value-of-Data-Summary.pdf.

105. Ibid.

106. Ibid.

107. Goldfarb and Tucker, "Privacy Regulation and Online Advertising."

108. "IAB Internet Advertising Revenue Report" (Interactive Advertising Bureau, April 2015), accessed July 23, 2019, https://www.iab.com/wp-content/uploads/2015/05/IAB_Internet_Advertising_Revenue_FY_2014.pdf.

109. "IAB Internet Advertising Revenue Report" (Interactive Advertising Bureau, May 2019), accessed July 23, 2019, https://www.iab.com/wp-content/uploads/2019/05/Full-Year-2018-IAB-Internet-Advertising-Revenue-Report.pdf.

110. McQuinn and Castro, "A Grand Bargain on Data Privacy Legislation for America."

111. Ibid.