A GRAND BARGAIN ON DATA PRIVACY LEGISLATION FOR AMERICA

ALAN MCQUINN AND DANIEL CASTRO
JANUARY 2019

ITIF
INFORMATION TECHNOLOGY & INNOVATION FOUNDATION
ITIF.ORG

Table of Contents

A Grand Bargain on Data Privacy Legislation for America

By Alan McQuinn and Daniel Castro

There is a growing chorus of voices calling for national data privacy legislation in the United States. Not surprisingly, stakeholders have offered competing visions for what such a law should look like. Designing data privacy legislation involves a complex process that must address a wide array of legal and regulatory issues. To help policymakers understand and evaluate these issues, this report compares how different laws and frameworks around the world address various data privacy issues; describes 30 components included in existing laws, frameworks, and legislative proposals; and explains each one's likely impact on consumers, businesses, and the digital economy. On the basis of this analysis, the report calls for a bold new privacy framework that expands and simplifies consumer data privacy rights, reduces compliance costs from existing state and federal regulations, and paves the way for more data-driven innovation. Specifically, the report calls for comprehensive data privacy legislation to repeal and replace existing federal privacy laws with a common set of protections, preempt state laws, improve transparency requirements, strengthen enforcement, and establish a clear set of data privacy rights for Americans based on the sensitivity of the data and the context in which it is collected.

The United States does not have a single federal data privacy law. Instead, it has multiple federal and state laws that regulate the private sector, often focusing on particular sectors or types of data, with multiple regulatory authorities responsible for oversight.[1] Where there are no sector-specific rules, the U.S. government provides oversight of industry self-regulation, allowing particular industry sectors to use voluntary agreements, peer pressure, and other methods to coordinate behavior without violating antitrust rules.[2] For example, the online ad industry has developed a robust self-regulatory program, and companies who commit to this program and violate its rules can face action by the Federal Trade Commission (FTC).[3] This arrangement has been one factor enabling the United States to be the world leader in innovative digital services. Of the 15 largest digital firms in the world, all are either American or Chinese.[4] In contrast, other economies with strict data protection regulations, such as the European Union, have fallen by the wayside in part because it is so hard to use data for innovation. Indeed, of the top 200 digital firms, only 8 are European.[5]

If Congress passes data privacy legislation, its key task will not be to maximize consumer privacy, but rather to balance competing goals such as consumer privacy, free speech, productivity, U.S. economic competitiveness, and innovation. It is relatively easy to pass legislation to maximize consumer privacy. Indeed, the Europe Union did just that when it created the General Data Protection Regulation (GDPR)—a set of strict data protection rules for EU member states—which went into effect in May 2018.[6] But this regulation came at a steep price: high compliance costs that were passed on to consumers; reduced choice in the digital economy

as some firms choose not to provide services; and limited innovation as it becomes much more difficult for organizations, including nonprofits, to use data to innovate and improve services.

Crafting privacy legislation that balances key goals is more difficult, both conceptually and politically, but it is essential if policymakers do not want to derail the continued success of the U.S. digital economy. Crafting such legislation requires a thorough understanding of the direct and indirect implications of various data protection policies. Policymakers who ignore the complexity of complying with privacy laws or the hidden costs of these regulations risk creating rules that undermine the digital economy by restricting the overall digital ecosystem and the benefits it provides consumers.[7] The goal of data privacy legislation should therefore not be to myopically maximize consumer privacy, but to maximize consumer welfare. In other words, consumer welfare involves privacy, but it also involves lower prices (or free products and services) and the development of new products and services. This approach requires finding the optimal level of regulation for the digital economy, with rules that are neither too weak nor too strong.[8]

This report focuses on potential federal data privacy legislation for private-sector data processing. It does not address government access to data or restrictions on government use of data. It proposes a grand bargain, in which Congress repeals existing federal data privacy laws, such as the Health Insurance Portability and Accountability Act (HIPAA) and Gramm-Leach-Bliley Act (GLBA), and replaces them with a single federal data privacy law that preempts state laws. The new federal law would establish a common set of federal protections for all types of data based on the sensitivity of the data and the context in which it is collected. This report also proposes to improve consumer protections by enhancing transparency requirements for business practices, and, establishing a set of clear basic rights for Americans. This report also proposes improving enforcement by granting regulators the appropriate authority to update and enforce rules while ensuring they have the proper constraints to protect industry from regulatory overreach and overzealous enforcement. In this way, its proposals will incentivize companies to focus less on check-the-box compliance and more on reducing actual consumer harm. This report also looks beyond U.S. borders, proposing how a data privacy law could facilitate data sharing abroad without simply acceding to demands from other countries or regions on how to protect data. And most importantly, it offers recommendations for how federal data privacy legislation can promote innovation and beneficial data collection, use, and sharing to ensure consumers continue to benefit from the growing digital economy, including services supported by targeted digital advertising.

The Push for U.S. Federal Data Privacy Legislation

Since the emergence of the World Wide Web, policymakers have understood that data privacy is important, but have differed over the right framework. Ira Magaziner's 1999 "Framework for Global E-Commerce," developed for President Clinton, recognized the important of privacy, but warned against a heavy-handed regulatory approach that could stifle the emerging digital economy. Magaziner wrote:

> "One of our fundamental values is that people should have the ability to protect their own privacy. And we believe that the use of the Internet as a medium will reach its full potential only if people feel comfortable online, only if they believe that their privacy is protected. However, we do not favor the European approach of trying to protect privacy by setting up government privacy boards and very elaborate regulations. Instead, we favor an approach where industry and consumer advocacy groups take the lead in forming codes of conduct to protect privacy."[9]

Congress has since regularly considered the issue, introducing several bills to establish a general set of rules that would apply to all data, not just information already protected by sector-specific laws. There was a flurry of legislative proposals in the early 2000s.[10] In the 106th Congress, Sens. Conrad Burns (R-MT) introduced the Online Privacy Protection Act (OPPA) of 1999 to fill gaps left by the Children Online Privacy Protection Act (COPPA) by requiring websites to notify users of how their information was being used and offer them a consent mechanism to limit that disclosure.[11] Similarly, Sens. John Kerry (D-MA) and John McCain (R-AZ) introduced the Consumer Internet Privacy Enhancement Act (CIPEA) in 2000, which required websites to provide notice and the ability of consumers to opt out of having their personally identifiable information (PII) collected.[12] The bill also allowed website operators to deny service to users if they opt out of providing their PII. In the 106th Congress, Sen. Earnest Hollings (D-SC) introduced a more-restrictive version of the OPPA, which would have prohibited online personal data collection without affirmative consent.[13] In the 107th Congress, Reps. Anna Eshoo (D-CA) and Chris Cannon (R-UT) reintroduced CIPEA in the House.[14] These efforts did not gain any traction. Later, in 2011, Senators Kerry and McCain again introduced privacy legislation, the Commercial Privacy Bill of Rights Act, which proposed rules that would give Americans the right to opt out of data collection and establish a requirement that companies post their privacy policy online.[15]

The executive branch has also proposed data privacy legislation. In 2012, the Obama administration proposed a "Consumer Privacy Bill of Rights," which would have defined a set of consumer privacy rights, such as focused collection and transparency, developed enforceable codes of conduct, strengthened FTC enforcement, and attempted to achieve interoperability with international privacy frameworks by establishing a safe harbor through enforceable codes of conduct.[16] This effort ended when Congress showed little appetite for sweeping new regulations.[17]

Recently, following several high-profile cases of data breaches and data misuse, as well as the Europe Union enacting GDPR and California passing a major privacy bill that has national implications, some U.S. policymakers have renewed calls for comprehensive data privacy legislation, with many wanting to import European rules. For example, when serving in the House of Representatives, Sen. Marsha Blackburn (R-TN) introduced the BROWSER Act in 2017, which would have mandated stricter levels of consent for certain categories of data, such as financial information, health information, the information of children under the age of 13, web browsing history, and more.[18] Sens. Ed Markey (D-MA) and Richard Blumenthal (D-CT) introduced the Customer Online Notification for Stopping Edge-provider Network Transgressions (CONSENT) Act that would regulate how online companies collect and share user data, mandating affirmative consent for data collection and use, compelling providers to serve even those consumers who do not give consent, and requiring data security practices and data breach notification.[19] Similarly, Sens. Amy Klobuchar (D-MN) and John Kennedy (R-LA) introduced the Social Media Privacy Protection and Consumer Rights Act of 2018 that would create disclosure requirements and enable users to opt out of collection and use of their data, as well as provide for certain user rights, such as the right to access, and more.[20] Reps. Suzan DelBene (D-WA) and Hakeem Jeffries (D-NY) introduced the Information Transparency and Personal Data Control Act, which would create transparency requirements; establish two categories of data, sensitive and nonsensitive personal information; mandate stricter protections for sensitive personal information, such as opt-in consent; and give extra powers to the FTC to enforce privacy rules.[21] Sen. Ron Wyden (D-OR) introduced the Consumer Data Protection Act of 2018 that would cement privacy protections into federal law, such as the "Do Not Track" measure for web traffic, and impose strict penalties for violations, such as a fine that could equal up to 4 percent of total annual revenue and 20 years in prison.[22] Sen. Brian Schatz (D-HI) introduced the Data Care Act of 2018, which would require providers to protect user data, prohibit providers from using user data in

ways that harm them, and give the FTC additional rulemaking authority.[23] The Trump administration has also gotten involved, with the National Telecommunications and Information Administration (NTIA) proposing guiding principles around the administration's approach to privacy.[24]

Some states, tired of waiting for national legislation, have also decided to legislate. In June 2018, California passed the California Consumer Privacy Act, which created a number of data privacy rights for consumers, such as the right to know what information businesses have collected about them and how that information is being used, the right to opt out of allowing businesses to share their data with third parties, and the right to have their personal information deleted.[25] Notably, this legislation also requires companies to treat all consumers the same, even if they opt out of data collection—a provision that creates a free-rider problem that undercuts the ad-supported digital economy.[26] In May 2018, Vermont passed Act 171 that created special rules for data brokers, which buy and sell user data, requiring them to register in the state and create comprehensive data security programs.[27] Nevada and Minnesota have passed privacy legislation to control how Internet service providers retain and share consumer information.[28] And several states have created privacy rules for specific technologies. For example, Illinois, Washington, and Texas have all created privacy laws requiring companies to obtain consent for processing biometric data.[29] And several states have passed laws related to privacy and the use of drones.[30] In fact, about half the states considered measures in 2018 to regulate Internet privacy.[31]

Moreover, companies such as Google, Verizon, and Charter; trade associations, including the Business Roundtable, the Internet Association, the Information Technology Industry Council, and the U.S. Chamber of Commerce; and advocacy groups such as the Electronic Frontier Foundation, the Center for Democracy and Technology (CDT), and Access Now have offered their own privacy principles.[32] CDT has gone further and offered draft legislation to codify its principles.[33]

THE RELATIONSHIP BETWEEN PRIVACY REGULATIONS AND INNOVATION

Policymakers considering data privacy legislation should balance consumer privacy protection with innovation. Privacy and security protections are important because rules that are too weak can make users feel uneasy about adopting technologies and services. However, beyond a baseline of protections, stronger privacy protections do not translate into more digital trust and therefore more digital adoption and use.[34] Policymakers getting this balance wrong can deter innovation and harm consumers because overly stringent regulation raises costs and reduces the relative quality of digital technologies, thereby negatively impact the people who use them.

Policymakers should also be cognizant of the fact that privacy regulations are not free. Stronger rules raise compliance costs and reduce revenues for companies that provide online services, which ultimately hurts consumers. Regulations that reduce the effectiveness of online advertising reduce the revenue digital companies can earn from the online ads that underpin much of 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 companies can only use data after obtaining affirmative consent from users, significantly harm advertising-based business models.[35] Higher costs with lower revenues reduce the investments companies can make to improve their online services. Companies may try to compensate by raising costs for consumers, such as by switching from providing free services to charging for them. This can make it more difficult for online companies, including start-ups, to monetize user engagement and stunt digital growth and adoption. Therefore, by making users pay for services

and reducing the capital companies can invest to make their products better, these types of regulations can actually reduce overall consumer welfare.

We have already seen these deleterious effects, such as when Europe adopted GDPR. Prior to its enactment, reports and surveys estimated its negative impact. For example, one 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.[36] Similarly, a 2016 study found that GDPR requirements for public authorities and companies to process personal data could result in companies needing to hire an additional 75,000 workers to comply with the law.[37] These effects played out after GDPR went into effect—hundreds of websites stopped servicing Europe entirely, and demand for online ads in Europe plummeted by between 20 and 40 percent.[38] Indeed, as of December 4, 2018, over 1,129 U.S. news sites were still not available in the European Union due to these rules.[39] Furthermore, GDPR is expected to affect the deployment of emerging technologies. For example, a 2017 Center for Data Innovation report argued that by raising the legal risks of companies developing and using artificial intelligence (AI), GDPR will have a negative impact on the development and use of AI in Europe.[40]

Before the adoption of GDPR, Europe had more stringent privacy laws than the United States which, according to scholarly research, held back Europe's digital ecosystem. Goldfarb and Tucker found that EU privacy regulation has decreased the effectiveness of online advertising, thereby reducing the revenue of websites that rely on ad-based business models.[41] Campbell et al. found that regulations like those adopted by the European Union not only impose costs on all firms, they disproportionally impact small and new firms.[42] In 2013, Christensen et al. also found that EU privacy regulations were particularly costly for small and medium-sized enterprises, costing them between €3,000 and €7,200 (roughly $3,400 and $8,000, respectively) per year, or 16 to 40 percent of IT budgets.[43] Further, a 2011 survey found that 63 percent of EU venture capital (VC) investors believed that an active opt-in privacy requirement would deter investment in Internet companies dependent on advertising revenue.[44] Another study found that in the European Union, VC investments into online news, online advertising, and cloud computing increased at a slower pace than in the United States, after the passage of the 2002 EU e-Privacy Directive. VC investment across these three sectors was between 58 to 75 percent lower than it otherwise would have been if the European Union and United States had maintained similar trends in investment beyond 2002.[45] The EU privacy rules are also one reason why, from 2012 to 2017, digital advertising expenditures grew more slowly in the European Union (93.5 percent) than in the United States (140.4 percent).[46] If EU digital ad revenue had grown at the same rate as in the United States, an additional €11.6 billion ($13.2 billion) would now be flowing annually to the European digital ecosystem, including to European Internet start-ups and publishing companies. To give a sense of the scale, in 2018, mobile app revenues paid for by advertising in Europe was an estimated €8 billion ($9 billion).[47]

Certainly, Europe's problems with lagging development and adoption of digital technologies have existed for decades, and were caused by many factors, including the lack of a digital single market. But stringent data privacy rules that limit innovation also played a role.[48] The United States should learn from Europe's mistakes and avoid following in its footsteps.

Principles for Federal Data Privacy Legislation

As ITIF has shown before, there is an optimal level of regulation for the digital economy—a Goldilocks level—with rules that are neither too weak nor too strong.[49] Policymakers can misapply each of the components discussed in this report in a way that does not achieve the right balance between protecting consumers and enabling innovation.

To both protect privacy and ensure innovation can proceed apace, Congress and privacy regulatory agencies should be guided by ten principles.

First, and most importantly, federal privacy legislation should **protect and promote innovation**. There is a reason this report later recommends rejecting several components in any federal privacy legislation, including an opt-in requirement for nonsensitive data, data minimization, purpose specification, right of deletion or to be forgotten, data retention limitations, privacy-by-design requirements, privacy personnel requirements, and private right of action. Overly restrictive and badly designed data protection laws usually result in less access to data or significantly constrain how it can be used—both of which limit innovation. If organizations are to face significant constraints on the data they can collect and the analysis they can do on that data, there should be no ambiguity as to what the result will be: higher costs, less revenue, less innovation for companies; and higher prices, less choice, and lower-quality services for consumers.

To ensure federal data privacy legislation does not harm innovation, Congress should consider both the direct costs (discussed in detail in a later principle) such as compliance and fines, and indirect costs such as reduced productivity, loss of competitiveness, and other second-order effects. In addition, policymakers should specify which metrics—such as the number and size of data breaches, the amount of financial fraud from identity theft, the number of identity theft complaints, and the level of consumer privacy concerns in federal surveys—legislation will target, and commit to revising legislation that fails to meet those thresholds after a reasonable period of implementation. Without a clearly specified vision of what a successful privacy outcome would look like, a new set of data privacy rules might simply create higher costs and more market uncertainty that reduces innovation and competitiveness.

In addition to avoiding bad policies, promoting innovation also means incentivizing continuous improvement in terms of privacy-enhancing policies and technologies. Frequently, companies iterate on their privacy policies and technologies over time to improve the overall consumer experience, so the framework should be flexible in its rules and enforcement to allow companies to continue learning, and to improve consumer privacy.[50]

Second, federal privacy legislation should **create a single set of data privacy rules for the United States**. Consumers should have the same protections regardless of which state they live in, and companies should not be faced with 50 different state laws. This will require federal privacy legislation to preempt state and local government privacy rules, including preempting their ability to add additional protections on top of federal rules for general data processing. This principle does not mean states should completely sit out of the process. States can exercise their authority, such as by providing addition oversight efforts through state attorneys general.

Third, federal privacy legislation should **create a common set of federal protections for all types of data**. This will mean removing duplicative or conflicting rules. To accomplish this, federal privacy legislation should sunset other sector-specific privacy laws, such as GLBA, HIPAA, and the Family Educational Rights and Privacy Act (FERPA), and bring the industries covered by those rules under a single federal data privacy law.

Importantly, this legislation should keep current sector-specific regulators for entities covered under these rules and enable these industries to use their current processes to comply with the new rules so as not to force expensive new compliance regimes on them.

Fourth, federal privacy legislation should **create data protection rules based on both the type of data and the type of entity collecting the data**. Federal privacy legislation should make a distinction between sensitive and nonsensitive personal data as well as data collected on behalf of a critical service versus a noncritical service. Critical services include services essential to an individual's safety, health, and economic well-being, such as banking, utilities, health care, and Internet access. Data that is both sensitive and collected as part of a critical service should be subject to the highest data protection requirements; data that is one, but not both, of these criteria should be subject to a lower level of requirements, and those that involve nonsensitive data for noncritical services should be subject to the fewest obligations.

Regarding enforcement, regulators should use a risk-based standard for determining the severity of enforcement actions for regulatory violations, focusing on harm and intent. Using a risk-based approach will ensure protections given to different categories of data reflect the actual risks associated with the collection of those types of data.

Fifth, federal privacy legislation should **enable consumers to make more informed decisions about how they share their personal data** through increased transparency in business practices. One of the hallmarks of the U.S. data privacy framework has been, in the absence of sector-specific rules, a notice-and-choice regime that allows consumers to choose whether to use a service based on an organization's stated privacy practices. While many consumers choose "rational ignorance," there is still room for improvement on the traditional privacy notices for privacy-sensitive consumers. Federal privacy legislation should mandate regulators work with industry to develop a machine-readable format to share an organization's privacy and security policy information electronically. This would allow apps to interact with this information, both to automate consumers' privacy preferences in software (such as a browser that notifies users whenever they visit a website that does not conform to their privacy preferences) and to allow consumers the ability to review this information through third-party apps and services.

Sixth, federal privacy legislation should **establish clear consumer rights**. These should include the right to opt out of having one's nonsensitive personal data collected by a critical service, or one's sensitive data collected by a noncritical service; the right to not have one's personal data collected or used by organizations that provide a critical service unless one opts in; the right to access; and the right to data portability. The latter two rights should have reasonable limits, such as on the costs organizations should have to bear to comply with requests and allowing organizations to recover their costs in some circumstances.

Seventh, federal privacy legislation should **address concrete consumer harms, rather than hypothetical ones.** This means considering specific steps to target the harms consumers are most likely to face, such as identity theft, discrimination, and credit card fraud. Unfortunately, many of these harms are only tangentially related to the ongoing debates about the private sector's collection and use of consumer data for online advertising because many of those pushing for federal privacy legislation tend to focus on legal and beneficial uses of data, rather than actual solutions that prevent tangible harms. Therefore, policymakers will need to consider additional measures beyond the data security programs and data breach notification standards discussed in this report.[51] For example, Congress should phase out the use of Social Security numbers and replace them with a secure alternative.[52] Congress should also address concerns about unlawful discrimination by

conducting a review of civil rights protections and closing any gaps in laws or enforcement capabilities. Many of these ideas are not privacy specific, nor have they been introduced as components of any previous or proposed privacy law or framework, and as a result are not addressed in depth in this report.

Eighth, federal privacy legislation should **minimize compliance costs for U.S. organizations**. If policymakers ignore costs entirely in favor of maximizing privacy, they risk creating rules that overly limit the private sector and offer little to no privacy benefit. For example, GLBA requires financial entities to send paper privacy notices to their consumers at enormous cost. By simply switching to electronic notices, these businesses could save an estimated $700 million annually without leaving users worse off.[53] Policymakers following this principle should use federal privacy legislation to eliminate all paper privacy notice requirements. Similarly, GDPR created a requirement for businesses to designate a data protection officer to fulfil user requests and do compliance.[54] While privacy advocates may cheer the influx of new jobs, the employee costs of hiring a privacy-compliance-specific officer restrict companies from using that money to improve their products and services, thereby leaving users worse off. Furthermore, forcing companies to obtain consent for trivial purposes unnecessarily raises costs without substantial consumer benefit.

Ninth, federal privacy legislation should **improve enforcement**. The FTC should continue to be the primary U.S. privacy enforcement agency.[55] Assuaging consumer fears will mean beefing up current enforcement missions, such as by targeting fraud and identity theft, but also by improving privacy enforcement. However, to accomplish this mission, the FTC will need more resources and expanded authority.[56] Regarding resources, the FTC has been woefully under-equipped for some time. Since 2010, the Commission's funding has fallen 5 percent when adjusted for inflation.[57] The FTC needs additional funding to pursue privacy and security cases, and hire more staff with this expertise. Moreover, the FTC needs expanded authority to extract meaningful fines from companies that intentionally mislead consumers or violate their privacy in ways that cause concrete harms. And federal privacy law should give the FTC the authority to conduct limited rulemakings for data privacy through its public processes, and act against companies that knowingly violate them. However, the legislation should be very specific in how the FTC can flex this ability to constrain the agency from creating rules beyond what Congress intends and to ensure such rules follow the above principles by considering their impact on innovation and addressing concrete harms. Federal privacy legislation can do this by ensuring the FTC not only considers the economic consequences of its enforcement actions, but also that it pays attention to harm and intent when using its enforcement authority against companies.[58]

Finally, federal privacy legislation should **promote international interoperability**, but not simply accede to demands from other countries or regions. Countries around the world are considering local data privacy laws, and the United States government should ensure its adopted privacy rules work with potential trade agreements, such as the United States-Mexico-Canada Agreement (USMCA), and intergovernmental privacy frameworks it has signed onto, such as the Asia-Pacific Economic Cooperation (APEC) privacy framework. However, if Congress passes the kind of privacy legislation proposed here, administrations should not accept other nations' false claims that U.S. privacy law is not robust or somehow fails the EU's adequacy tests—claims other nations use to justify cutting cross-border data flows. Such rhetoric and actions should be seen for what they are: barriers to free trade.

Moreover, the United States should not stand by while other countries adopt privacy rules that affect U.S. competitiveness. Indeed, other regions, such as the European Union, have actively sought to expand their regulatory model, particularly GDPR, to other countries through both advocacy and enforcement of the rules themselves—advocating a false narrative that many have bought into that GDPR is pro-innovation. This

strategy has been successful. For example, Colombia issued rules that copied GDPR's approach to international data flows in 2017.[59] To push back on badly designed frameworks and ensure international interoperability, U.S. privacy legislation should direct the executive branch to vocally and forcefully advocate for the new U.S. approach to data privacy abroad. Legislation should direct the U.S. government to do this through bilateral agreements, such as those established in the Clarifying Overseas Use of Data (CLOUD) Act, through trade agreements, and in international multistakeholder forums.[60] It should expand the State Department's digital attaché program and ensure more State Department foreign service officers understand the different international approaches to data privacy and the advantages of the U.S. approach.

COMPONENTS OF PRIVACY LAWS

There are many different ways to design privacy laws, and the decisions about which types of provisions to include and how the law will address them can have a significant impact on consumers, organizations, and the overall economy. This report describes the various components found in the most significant privacy laws and frameworks, the impact different ways of addressing these components can have on consumers and businesses, and how the United States should address these items in federal legislation.

The report reviews Europe's GDPR, California Consumer Privacy Act (CCPA), the Obama administration's proposed Consumer Privacy Bill of Rights (CPBR), the Organization for Economic Cooperation and Development (OECD) Core Privacy Principles, and APEC privacy framework.[61] We also describe three key U.S. laws—HIPAA, GLBA, and FERPA—to show how U.S. privacy law treats some of the most sensitive consumer, health, financial, and education data, respectively.[62]

Some laws contain provisions not found in most other laws. For example, CCPA establishes a consumer privacy fund for state-led investigations into potential violations. We omitted these types of one-off provisions from our analysis and focused on components most likely to be considered in federal legislation.

To that end, we assessed the following 30 components:

- Scope
- Preemption
- Rescission
- Definition of Personal Data
- De-identified Data
- Publicly Available Data
- Definition of Covered Entity
- Method of Consent
- Non-Consent-Based Data Processing
- Transparency
- Right of Access
- Data Portability
- Right to Rectification
- Right to Deletion and Right to be Forgotten
- Data Retention
- Data Transfers to Other Countries
- Incentives and Penalties to Sharing Data
- Privacy by Design
- Privacy Personnel
- Data Security Program
- Data Breach Notification
- Data Minimization
- Purpose Specification
- Jurisdiction
- Harm Focus
- Oversight
- Rulemaking Authority
- Penalties
- Privacy Complaints
- Private Right of Action

1. Scope

Privacy laws and frameworks can apply to certain types of records collected by certain entities, or broadly apply to all forms of data and organizations. Rules can either be narrowly scoped to address certain types or formats of information, such as regulations specific to digital health records collected by hospitals, or broadly worded to apply to paper records, digital records, physical recordings, and more collected by every variety of business. For example, GDPR, APEC, OECD, and CCPA apply broadly to all personal information, not just a specific type of information collected by specific types of organizations.

Table 1: Scope

Framework	Scope
GDPR	Uses broad definition of personal data that encompasses all forms and mediums gathered by all types of organizations.
APEC	Uses broad definition of personal data that encompasses all forms and mediums gathered by all types of organizations.
OECD	Uses broad definition of personal data that encompasses all forms and mediums gathered by all types of organizations.
HIPAA	Specifically applied to health information transmitted or stored in any form or medium by health-care providers.*
GLBA	Applies to all forms of information not already made public that are provided to financial services companies in the course of conducting business.
FERPA	Applies to all forms of education records maintained by education institutions.
CCPA	Uses broad definition of personal data that encompasses all forms and mediums gathered by all types of organizations.
CPBR	Uses broad definition of personal data that encompasses all forms and mediums gathered by all types of organizations.

*** The HIPAA security rule does not apply to paper records, but the privacy rule does.**

Impact

Policymakers who do not consider scope when they create rules for data may not necessarily realize their pervasiveness. Broadly scoped rules usually apply to every form of personal information, and therefore affect every type of business. For example, GDPR, CCPA, and CPBR created or proposed rules that would affect grocery stores or chain movie theaters just as much as they would impact large social media platforms, advertisers, and businesses that sell data. Depending on how strict they are and the scale of the fines they propose, these rules can create large costs and market barriers for entities of all kinds.

Recommendation

Federal privacy legislation should scope its rules to apply to all data and should not treat digital data in a different way from other forms of data. If privacy protection is the goal, a broad scope is important because privacy risks are not confined to data that is entered digitally. Moreover, having a standard for digitally collected data that is different for data collected in other ways (e.g., over the telephone, collected on a paper

form, scanned from a driver's license, etc.) is unfair and discriminatory. However, policymakers should be aware that extending a privacy regulation to all kinds of data will significantly increase compliance costs and complexity, in part because the scope of offline data collection is massive and the costs of providing notice, choice, redress, and other consumer measures is much higher for offline than online applications. The only way to square the circle between broad-based coverage and limited economic cost is to ensure privacy regulations are designed to limit the compliance burden.

2. Preemption

Preemption allows the federal government to prevent state and local governments from passing competing or contradictory privacy laws that may confuse consumers and increase compliance costs for organizations. These laws can prevent state and local governments from creating rules, enforcing rules, or both. Some laws can create a ceiling for state and local government regulations. For example, GLBA preempts state and local governments from passing additional privacy rules for banks but does not prevent state AGs from enforcing its rules.[63] And GDPR sets binding rules for all EU member states and enables them to enforce these rules.[64] In contrast, some laws only set a floor for rules. For example, HIPAA and FERPA establish certain baseline privacy requirements but do not preempt states from creating additional privacy laws.[65]

Table 2: Preemption

Framework	Preemption of Creating Rules	Preemption of Enforcement
GDPR	Yes*	No
APEC	No	No
OECD	No	No
HIPAA	No	No
GLBA	Yes	No
FERPA	No	Yes†
CCPA	N/A	N/A
CPBR	Yes‡	No

*** GDPR sets binding rules for all EU member states.**

† The main enforcement mechanism of FERPA is withholding funds, which is overseen by the Department of Education.

‡ CPBR only preempts states from creating laws for personal data processing, not all privacy rules.

Impact

Without federal preemption, state and local governments may create additional privacy laws that make compliance more complex for organizations and create contradictory requirements. States have done this before. For example, every state has its own data breach law.[66] Competing laws makes it more difficult to educate consumers about their privacy rights and makes compliance more complicated for organizations.[67]

Recommendation

Federal privacy legislation should set a national standard for consumer data protection and preempt state and local governments from passing their own laws that would add to or diminish from these protections. In other words, optimal federal legislation should set both a floor and a ceiling. This preemption should apply to all state data privacy laws, including data breach laws and state data privacy laws for specific types of information, such as biometric data. Policymakers should be wary of calls to only set a floor, because the inherently cross-border nature of the Internet means conflicting state laws could create confusion and raise costs for businesses and consumers. However, federal privacy legislation should still allow states to play a role in privacy enforcement, enabling state attorneys general to bring cases wherein data misuse has harmed a substantial number of a state's residents.

3. Rescission

Privacy laws can replace older laws or statutes to remove duplicative or outdated rules. For example, GDPR replaced the EU Data Protection Directive (Directive 95/46/EC) with a new set of rules, protections, and responsibilities for member states.[68] Other laws, such as CCPA and CPBR, only add new language without removing previous rules.

Table 3: Rescission

Framework	Rescission
GDPR	Replaces Directive 95/46/EC, which created differing implementations and applications across the EU member states.
APEC	N/A
OECD	N/A
HIPAA	No previous federal privacy law for health data; has been amended by subsequent laws.
GLBA	No previous federal privacy law for financial data; has been amended by subsequent laws.
FERPA	No previous federal privacy law for education data; has been amended by subsequent laws.
CCPA	Adds to California civil code and does not replace other state-enacted laws.
CPBR	Would amend the Federal Trade Commission Act, but does not replace any section therein.*

*** CPBR lists several federal law and sections of U.S. code that that it does not modify, limit, or supersede. This includes GLBA, HIPAA, the Privacy Act of 1974, and more.**

Impact

Removing duplicative, outdated, or contradictory language from U.S. code is a necessary part of passing a new law. Without removing contradictory legal requirements, businesses and regulators may find themselves complying with multiple laws seeking the same objective, thereby creating additional compliance costs with little value to consumers. However, replacing older regulatory requirements can generate costs for businesses that must amend their processes to comply with the new rules.

Recommendation

Federal privacy legislation should rescind existing privacy laws, such as GLBA, FERPA, HIPAA, COPPA, and others, and have all sectors and functions under one unified privacy regulation, with differences between them based on the sensitivity of the data and the degree of consumer choice in providing the data. To minimize business impact, Congress should establish a sunset period during which entities covered by existing sectoral privacy laws could continue to comply with the old rules before switching to the new ones. To limit this impact on both the public and private sector, policymakers should also ensure sector-specific regulators stay in place to oversee these changes and continue future enforcement.

4. Definition of Personal Data

Privacy laws and frameworks use different definitions of personal data, and these definitions impact what information a law covers. Some laws also make distinctions between "personal data" and "sensitive personal data," affording additional protections to the latter. In addition, some laws also make a distinction based on who controls the data. For example, FERPA only applies to certain personal data maintained by an educational agency or institution, and HIPAA only applies to personal data maintained by covered entities, such as health insurers and health-care providers.[69]

Table 4: Definitions of personal data

Framework	Definitions of Personal Data
GDPR	"Personal data" means any information relating to an identified or identifiable natural person who can be identified directly or indirectly with that information.*
APEC	"Personal information" means any information about an identified or identifiable individual.
OECD	"Personal data" means any information relating to an identified or identifiable individual.
HIPAA	"Protected health information" means individually identifiable health information that is transmitted or stored by electronic media or other medium.†
GLBA	"Nonpublic personal information" is provided to a financial institution to obtain a financial product or service, results from a transaction between the consumer and the institution involving a financial product or service, or is obtained in connection with providing a financial product or service.‡
FERPA	"Education Records" are directly related to a student and maintained by an educational agency or institution or by a party acting on behalf of an agency or institution.§
CCPA	"Personal information" means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a consumer or household.
CPBR	"Personal data" means any data that is under the control of a covered entity, not otherwise generally available to the public through lawful means, and is linked or linkable to a specific individual, or linked to a device that is associated with or routinely used by an individual.‖

*** GDPR excludes anonymized data from this definition.**

† This definition excludes individually identifiable information in education records protected by FERPA, de-identified data, employment records, government records, or a person dead over 50 years.[70]

‡ This definition does not include any information that is publicly available.

§ This definition does not include records kept in sole possession of the maker as a personal memory aid, records of a law enforcement unit of an educational agency or institution, or records relating to an individual who is employed by an educational agency or institution that are made during the course of business, related to the individual's capacity as an employee, and are not available for other purposes.[71]

‖ CPBR excludes de-identified data, deleted data, employee information, and cybersecurity data from this definition.[72]

Impact

In general, there are four types of personal data that can be used to distinguish or identify an individual or can be linked or are reasonably linkable to that individual.[73] The first category is observable information, which is personal information that can be perceived first-hand by other individuals. The second category is observed

information, which is information collected about an individual based on a third party's observation or provided by the individual but does not allow someone else to replicate the observation. The third type of information is computed information, which is information inferred or derived from observable or observed information. Finally, associated information is information a third party associates with an individual. Associated information, by itself and unlike the other three categories, does not provide any descriptive information about an individual (i.e., it does not describe qualities about an individual).

Definitions of personal data that are overly broad may force organizations to spend unnecessary resources protecting data, such as anonymized data with little to no privacy implications, that could be better spent elsewhere. By making the definition contingent on whether data is "linkable" or "identifiable" to an individual, GDPR, APEC, and OECD definitions will continue to encompass new types of information as new technologies and applications link data that previously was not considered personal to specific individuals. For example, engine performance data in a car may be linked to its driver, but this maintenance data has few, if any, privacy risks.

Different types of data have different levels of sensitivity and therefore different risks associated with them and how they are used. Some privacy laws use a broad definition that unnecessarily applies strict standards to less-sensitive data. Ambiguous definitions can also create regulatory uncertainty and thereby make compliance more difficult, although the definitions reviewed in this report do not create this uncertainty.

Moreover, some definitions also ignore the context in which the data is collected. For example, "health data" broadly defined could include anything from someone's highly sensitive medical records to a posting on social media about completing a marathon. Requirements to treat all information the same would be unnecessarily heavy-handed and limit consumer choice.

Recommendation

Federal privacy legislation should make a distinction between nonsensitive and sensitive personal data, as well as data collected as part of a critical service versus a noncritical service. Federal privacy legislation should define sensitive personal data as personally identifiable information that likely presents a high risk to individuals if made public, such as health-related data, genetic and biometric data, data regarding children under the age of 13, and precise geolocation information. Federal privacy legislation should also define critical services as those essential to an individual's safety, health, and economic well-being, such as banking, utilities, health care, and Internet access. For both definitions, federal privacy legislation should give the Federal Trade Commission the authority to determine which types of data and which service providers to classify under these definitions—and these determinations should be revised on a regular schedule.

The goal should be to create three levels of data protection—low, medium, and high—based on the sensitivity and risk of each type of data: nonsensitive personal data collected by noncritical services (e.g., movie preferences on a video streaming service); nonsensitive personal data collected by critical services or sensitive personal data collected by noncritical services (e.g., video preferences by an ISP based on network traffic analysis, or medical conditions by an e-commerce website based on analysis of everyday purchases); and sensitive personal data collected by critical services (e.g., health information by an ISP based on network traffic analysis). Each level would have distinct types of protections (for additional discussion, see section on opt-in versus opt-out consent).

5. De-identification

Privacy laws and frameworks can create special rules for de-identified data—wherein a covered entity uses special techniques to achieve a reasonable level of confidence the data cannot be used to infer information about, or otherwise be linked to, a particular data subject.[74] There are three main types of de-identification. When data is anonymized, it is irreversibly changed such that it can no longer be used to identify an individual. When data is pseudonymized, data controllers substitute the identity of the data subject with some other data, and additional information is required to reidentify the data subject. When data is aggregated, it is processed and expressed only in summary form.

Because de-identified data has significantly fewer privacy implications for individuals, most privacy laws create exemptions for some form of de-identified data. For example, OECD leaves the treatment of de-identified data up to member states.[75]

Table 5: Definitions of de-identified data

Framework	De-identified Data
GDPR	Exempts anonymized data from its definition of personal data; considers pseudonymized and aggregated data as personal data.*
APEC	Definition of personal data only applies to information that can be used to identify an individual.
OECD	Leaves the treatment of de-identified data up to member states.
HIPAA	Exempts de-identified data from its definition of health data; if the data is reidentified, HIPAA's protections apply.
GLBA	Exempts de-identified data from its definition of nonpublic personal data.
FERPA	Exempts de-identified data from the obligations is imposes on covered entities.
CCPA	Exempts anonymized and aggregated data from the obligations it imposes on covered entities; exemptions do not apply to pseudonymized data.†
CPBR	Exempts de-identified data from its definition of personal data.‡

*** GDPR encourages pseudonymized data use in its "privacy-by-design" components.[76] Moreover, it creates certain exemptions from obligations under the law for aggregated data used for statistical purposes.[77]**

† CCPA also requires de-identification or pseudonymization for information used in its "research" exemption.[78]

‡ CPBR says data is de-identified when it cannot be linked in a practical manner to the data subject; when the data controller publicly commits to not reidentifying the data; when the covered entity uses contractual or legally enforceable prohibitions on each entity it shares data with to not reidentify the data; and when those entities also publicly commit to not attempting to reidentify it.[79]

Impact

Sometimes organizations need access to identifiable personal data, while other times firms can use de-identified data. Because a number of de-identification techniques have been used inappropriately, some privacy advocates have opposed de-identification. However, de-identification is an important way to ensure firms have access to data while providing strong privacy protections to individuals. Moreover, de-identification techniques can be used effectively, and the public and private sector can reduce risks associated with reidentifying data by developing industry best practices for de-identification.[80]

Recommendation

Federal privacy legislation should exempt de-identified data, including anonymized, pseudonymized, and aggregated data, from both its definitions of nonsensitive and sensitive personal data. However, because de-identification is neither simple nor straightforward, policymakers should support the development of tools, training, and best practices so these techniques may be more widely adopted. In particular, federal privacy legislation should direct the National Institute of Science and Technology (NIST) to build upon its previous efforts and work with the private sector to develop a voluntary governance structure that enables organizations to continually assess the overall quality of their de-identified datasets to ensure their utility remains high, and the risk of reidentification remains sufficiently low.[81] And companies that de-identify data poorly—particularly sensitive personal data—so that it is later reidentified, should face potential penalties from the FTC.

6. Publicly Available Data

Some privacy laws and frameworks create special rules for personally identifiable data that is made public. Publicly available data can apply to data an individual knowingly permits to be available to the public or is made available to the public through government records, journalism, or other legal filings. For example, certain real estate information is required by U.S. law to be publicly available.

APEC, CPBR, and CCPA each have exemptions for information that is publicly available.

Table 6: Publicly available data

Framework	Publicly Available Data
GDPR	Does not exempt "publicly available data," but does require member states to abide by its rules governing freedom of expression and information, including journalistic, academic, artistic, and literary expression with the right to the protection of personal data under GDPR.*
APEC	Considers "publicly available information" to be personal information about an individual, which the individual knowingly makes or permits to be made available to the public, or is legally obtained and accessed from government records that are available to the public, journalistic reports, or information required by law to be made available to the public.
OECD	None
HIPAA	Protections do not apply to publicly available data.†
GLBA	Protections do not apply to publicly available data.†
FERPA	Protections do not apply to publicly available data.†
CCPA	Does not include publicly available information as part of "personal information," such as data lawfully made available from federal, state, or local government records.
CPBR	Does not apply certain protections, such as deletion and accuracy requirements, to information made public by the federal government or the individual.*

*** GDPR specifically says processing applies to all data made public by the data subject.[82]**

† These industry-specific rules apply to specific types of data controllers and not information in the public eye.

Impact

When information is already public, restrictions on the use of personal data have no impact on privacy. For example, consent requirements do not protect the privacy of personal information that is already made public by government records. Moreover, privacy laws that create exceptions for publicly available information help protect free speech, such as news reports that contain personal details.

Recommendation

Federal privacy legislation should create exemptions for publicly available information.

7. Definition of Covered Entity

Another important component of any data privacy law is to whom it applies. With certain sector-specific rules, such as HIPAA, GLBA, and FERPA, the law only applies to a small number of entities. For example, HIPAA only applies to health data used by health plans, health-care clearinghouses, and health-care providers. These laws may also make distinctions based on whether the organization controls the data it holds (i.e., a "data controller") or whether it is holding or processing the data on behalf of another organization (i.e., a "data processor"). Rules for data controllers tend to be stricter than for data processors.

Table 7: Definitions of covered entities

Framework	Definition of Covered Entities
GDPR	"Controller" means the natural or legal person, public authority, agency, or other body that determines the purposes and means of the processing of personal data; "Processor" means a natural or legal person, public authority, agency, or other body that processes personal data on behalf of the controller.
APEC	"Personal information controller" means a person or organization that controls the collection, holding, processing, or use of personal information. This definition includes persons or organizations who instruct another person or organization to collect, hold, process, use, transfer, or disclose personal information on their behalf.*
OECD	"Data controller" means a party who, according to domestic law, is competent to decide about the contents and use of personal data regardless of whether or not such data is collected, stored, processed, or disseminated by that party or by an agent on its behalf.
HIPAA	"Covered entity" means either a health plan, health-care clearinghouse, or health-care provider that transmits any health information in electronic form in connection with a covered transaction; "Business associate" means an entity that creates, receives, maintains, or transmits health information on behalf of the covered entity.
GLBA	"Financial institutions" engage in activities that are financial in nature or incidental to such financial activities.†
FERPA	The educational institution provides educational services, instruction, or both to students; or the educational agency is authorized to direct and control public elementary, secondary, or postsecondary educational institutions.‡
CCPA	A "businesses" is a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is operated for profit, collects personal information, determines the purposes behind and means of processing consumers' personal information, does business in the State of California, and satisfies one or more of the following thresholds: has an annual gross income over $25 million; buys, sells, or shares information of 50,000 or more customers, households, or devices; or derives 50 percent or more of its annual revenue from selling personal information.
CPBR	"Covered entity" means a person that collects, creates, processes, retains, uses, or discloses personal data from interstate commerce. There are a few exceptions to this definition.§

*** This definition excludes a person or organization that performs such functions as instructed by another person or organization, and organizations or individuals who collect, hold, process, or use personal information in connection with the individual's personal, family, or household affairs.**

† GLBA also defines "affiliates" and "nonaffiliated third parties" and designates that sharing information to these entities comes with different requirements, such as notice and consent.

‡ Regulations apply to educational institutions that receive federal funding.

§ Exceptions include governments; contractors of governments; natural persons acting in a non-de minimis commercial capacity; anyone collecting data on fewer than 10,000 individuals or has fewer than 5 employees that does not knowingly collect, use, retain or disclose information linked to personal data; anyone with 25 or fewer employees that would be a covered entity solely because of employee data; exceptions created by the FTC, and security-threat researchers.

Impact

Certain laws treat similar types of data differently depending on who gathers the data. For example, although health-care providers must abide by HIPAA, this law does not apply to other entities such as online companies or data brokers that also collect and use health data, unless they have a direct business relationship with a covered entity.[83] Many privacy advocates oppose this distinction because they believe all health data should have the high level of protection afforded under HIPAA. However, there is merit to treating data created in different context by different rules. For example, patient-doctor confidentiality is necessary for good treatment, and this information is needed by insurers to properly process health benefits, so it makes sense for there to be stronger privacy requirements imposed on these health-care providers and payers. However, if someone shares information about their health condition on social media, the individual clearly has a lower privacy expectation and the law should not impose the same standard.

Some laws exempt certain organizations from providing the same privacy protections as others based on their size. For example, CPBR-exempted companies that collect data on fewer than 10,000 individuals or have fewer than 5 employees and do not knowingly link that data to individuals.[84] This privacy exemption for small businesses rightly shows that privacy regulations result in costs for business and the economy, and that overly rigid and comprehensive laws can have a large effect. Moreover, in this case, exempting a class of organization based on size implies the privacy goal is not that important and has a negative impact on consumers.

Recommendation

Federal privacy legislation should impose certain requirements on data processors for both nonsensitive and sensitive personal data. These requirements should not allow exemptions for organizations based on their size (e.g., workforce, user base, or revenue). The reason is straightforward: If the main goal of federal legislation is privacy, individuals should have as much right to privacy when dealing with larger organizations as with smaller ones.

Federal privacy law should designate a subset of services provided by these covered entities as “critical services” that are subject to higher standards and requirements (as previously described in the Definition of Personal Data section). These services are essential to an individual’s safety, health, and economic well-being, and include but are not limited to utility services, financial services, health care, and Internet services.

8. Method of Consent

There are two ways privacy laws can give consumers choice over how others may use their information: opt-in and opt-out. Opt-in laws require organizations to obtain affirmative consent from individuals before they may use their information for all but the most narrow purposes (e.g., delivering a package). Opt-out laws require organizations to abide by requests from individuals to not use their data.

Often, opt-out requirements are coupled with transparency requirements that require organizations to disclose how they collect, use, and share personal information—a practice called notice and choice. Most companies with an Internet presence that collect personally identifiable data in the United States abide by notice and choice. [85] However, some sector-specific privacy laws have opt-in requirements. For example, FERPA requires organizations to obtain opt-in consent before disclosing educational records, and HIPAA uses both opt-in and opt-out consent mechanisms (depending on the use of health data).[86]

Most privacy laws have exceptions for when it is necessary to obtain consent. For example, GDPR allows data processors to use personal data without consent when they have "legitimate interests" in the processing of that data, such as for fraud prevention.[87] Others, such as HIPAA, GLBA, FERPA, CCPA, and CPBR carve out exceptions for gathering consent.

Table 8: Method of consent

Framework	Consent
GDPR	Opt-in consent.
APEC	Does not mention a consent mechanism.
OECD	Does not mention a consent mechanism.
HIPAA	Depends on the type of disclosure; opt-in consent is part of health "authorizations," which are required for marketing or sale of personal health information.*
GLBA	Opt-out consent.
FERPA	Opt-in consent.
CCPA	Opt-out consent.
CPBR	Does not specify mechanism for consent but does explain that covered entities must provide individuals with a means to withdraw consent that is reasonably comparable to the means used to grant it.

*** An authorization is a detailed document that gives covered entities permission to use protected health information for specified purposes.[88]**

Impact

Most privacy advocates push for opt-in because they do not believe individuals are sophisticated enough to make a choice on their own, and because they see little to no value in data collection. However, the differences in regime are striking in terms of the degree of data shared. Research suggests opt-in regimes frame consumer choices in a way that leads to suboptimal data sharing because most users select the default option—for a number of irrational reasons.[89]

Moreover, opt-in requirements have a negative impact on businesses, but do not provide greater privacy protections to consumers. First, obtaining affirmative consent to collect and use certain user data not only reduces the amount of data collected, but raises costs and reduces revenues, forcing organizations to pass these added costs or reduced revenues on to consumers in the form of higher prices or lower quality service.[90] In particular, opt-in rules make it more difficult for sites that use targeted online advertising to monetize free online services, thereby restricting market innovation and adversely affecting advertising-based online business models.[91] Opt-in rules also impose other burdens on consumers, such as unwanted calls and emails.[92]

In contrast, opt-out rules enable data sharing while still allowing the relatively small share of consumers with strong privacy preferences to choose not to share their data.

Recommendation

Federal privacy legislation should require organizations to provide notice for nonsensitive personal data used in noncritical services. In addition, organizations should be required to allow individuals to opt-out of data collection if they are providing a critical service collecting nonsensitive personal data or a noncritical service collecting sensitive personal data. Finally, businesses providing critical services and collecting sensitive personal data should be required to adhere to an opt-in standard. Covered entities providing both critical and noncritical services should be required to adhere to the consent requirements related to the type of service they are providing. For example, if Internet services were designated as a critical service, then an Internet service provider that also has a streaming music service would be required to obtain opt-in consent from any sensitive data collected in relation to providing broadband, and an opt-out consent standard for any sensitive data collected as part of its streaming music service.

Figure 1: Recommended consent mechanism based on sensitivity of data and type of service

	Noncritical Service	Critical Service
Nonsensitive Personal Data	No required choice mechanism	Opt-out
Sensitive Personal Data	Opt-out	Opt-in

9. Non-Consent-Based Data Processing

Privacy laws and frameworks can create special circumstances in which covered entities do not need to gather users' consent to collect or use personal information. They generally allow for non-consent-based data processing in two ways. First, some laws outline the specific circumstances under which covered entities have the right to process personal data (e.g., for national security reasons, with legitimate interest, with consent, etc.). For example, under GDPR, there are six justifications for covered entities processing data.[93] Besides consent, the five others are contract, legal obligation, vital interests of the data subject, public interest, and legitimate interests. Second, some laws outline specific exemptions under which covered entities do not need to gather consent to process personal data. For example, GLBA, FERPA, and CPBR specify conditions that do not require consent.

Table 9: Non-consent-based data processing

Framework	Non-Consent-Based Processing Requirements
GDPR	Non-consent-based processing is allowed for purposes related to contracts, legal obligations, vital interests of the data subject, public interest, and legitimate interests.*
APEC	N/A
OECD	N/A
HIPAA	Certain types of disclosure do not require any form of consent, such as uses and disclosures required by law for public health activities; victims of abuse, neglect, or domestic violence; health oversight activities; judicial and administrative proceedings; disclosures for law enforcement purposes; research purposes; to avert a serious threat to health or safety; or specialized government functions.
GLBA	Several exceptions to its consent requirements are offered, including protecting user confidentiality and preventing potential harm to persons holding a legal or beneficial interest relating to the consumer; to provide information to insurance rate advisory organizations or consumer reporting agencies; to comply with federal state or local laws; and to respond to authorized civil, criminal, or regulatory investigations or judicial processes.
FERPA	There are several exemptions, such as for legitimate educational interests and to comply with investigations or judicial orders.†
CCPA	There are several exemptions, such as when the information is necessary to complete the transaction or is needed to comply with a legal authorization.‡
CPBR	Several "enumerated exceptions" are offered. These include preventing fraud; preventing child exploitation or serious violent crime; cybersecurity concerns; protecting the rights or property of the covered entity or, upon consent of the customer, the covered entity's customer; monitoring or enforcing agreements between covered entity and individual; processing customary business; or complying with a legal requirement or governmental request.

*** To be within the public interest, the use or collection of the data must be set out in EU or member state law, which may designate a particular data controller to carry out the function. For example, public interest can include reporting crimes, taxation, preventive or occupational medicine, public health or social care, and election campaigns.[94]**

† FERPA outlines several exceptions throughout the law, both in terms of uses by covered entities and for health and safety reasons.[95]

‡ California's attorney general will also establish other exceptions, such as when it is necessary to comply with state and federal laws.[96]

Impact

Sometimes certain data should be able to be shared and processed by covered entities to uphold national or public interests. For example, often in pursuant to investigations or judicial processes, law enforcement and national security agencies will need access to personal information. Importantly, many laws already restrict how and when public entities can access and use consumer data, such as the Privacy Act of 1974 and the Electronic Communications Privacy Act of 1986. (This report does not focus on regulations governing public-sector use of personal data or offer recommendations for how to improve those processes.)

Moreover, without public interest exceptions, privacy laws can limit important uses of data, such as medical research. For example, a previous draft of GDPR required researchers to reuse data or perform follow-up studies to obtain consent from each patient in the original study.[97] This would have created burdensome hurdles for researchers that were logistically difficult and sometimes completely infeasible.

Recommendation

Federal privacy legislation should create specific non-consent-based exceptions to the collection and use of both sensitive and nonsensitive personal information. These exceptions should include public or national interests. Relevant federal agencies, such as the Department of Justice, the Department of Commerce, and the FTC, should work together to set the standards for declaring certain use cases as within the public or national interest, including but not limited to national security, law enforcement, and public health.

10. Transparency

Privacy laws can mandate organizations disclose to consumers how their information is used, the purposes for which it is used, with whom is it shared, other information related to contacting the covered entity, users' rights under the law, and the covered entity's legal duties. Each privacy law or framework we examined has a transparency component.

Table 10: Transparency

Framework	Transparency Requirements
GDPR	When personal data is collected, data controllers should disclose several types of information, such as the identity and contact information of the data controller, the purposes of the processing, the period of time the data will be stored, the existence of rights guaranteed to data subjects under GDPR, and more.*
APEC	Data controllers should provide clear and easily accessible statements about their privacy practices and policies, including the fact that personal information is collected, the purposes for which it was collected, types of organizations to which it might be disclosed, the identity and location of the data controller, and the choices and means individuals have for limiting their disclosure or use of this data.
OECD	There should be a general policy of openness about developments, practices, and policies with respect to personal data. Consumers should be able to obtain information about whether the controller has access to personal data, the purposes of its use, as well as the identity and usual residence of the data controller.
HIPAA	Consumers have the right to adequate notice of the uses and disclosures of health information by the covered entity, individuals' rights, and the covered entity's legal duties.†
GLBA	Requires covered entities to provide consumers with an initial notice of privacy policies and practices when the customer relationship is established.
FERPA	Requires companies to provide to consumers an annual notice with their rights under the law, including consent to disclosures of personally identifiable information contained in students' education records.
CCPA	Data controllers that collect consumers' personal information are required to disclose the categories and specific pieces of personal information to that consumer at or before the point of collection.
CPBR	Each covered entity shall provide individuals in concise and easily understandable language, accurate, clear, timely, and conspicuous notice about the covered entity's privacy and security practices, and any updates or modifications to such notice.

*** GDPR has many notice and disclosure requirements for personal data collection and use.[98]**

† There are two exceptions to this notice requirement: a group health plan that does not create or receive protected health information, and inmates at correctional institutions that are covered entities.[99]

Impact

Transparency components are essential to privacy legislation because they both keep users informed and enable regulators to better hold companies accountable for their actions.[100]

Ironically, to comply with transparency requirements, many privacy policies are quite long and not written in plain language. Instead, most are written for lawyers rather than consumers because doing otherwise could expose companies to penalties for noncompliance. If companies make even a simple mistake or omission, they risk being penalized by regulators such as the FTC.[101] However, these user agreements do not need to be simplified because competitors as well as consumer groups, such as the Electronic Frontier Foundation, highlight problems they discover in companies' terms of service. Moreover, if policies are machine readable, organizations can develop third-party tools to "translate" them into easy-to-understand information.

Recommendation

Federal privacy legislation should require organizations to disclose to consumers the information they collect, store, and share about them. The FTC should work with industry to develop a machine-readable format to share this information electronically that can be displayed in a clear and simple way to consumers—as well as to third parties—such as through search engines or browsers.[102] Companies should be able to comply with this requirement by posting information on their website, even if the only interaction with the customer is by mail or in person. In addition, this transparency requirement should eliminate the need to provide paper privacy notices.

However, when creating standard privacy notices, policymakers should avoid pop-up notices or interstitials that require users to click through to give their consent. For example, the European Union has experimented with notice requirements for web browser cookies, and those rules have resulted in high user costs with little to no privacy benefit.[103]

11. Right of Access

The right to access requires organizations to provide individuals, upon request, a copy of their personal data and other supplementary information. Right of access provisions typically state whether organizations may charge for this access and how long they have to respond to requests. In addition, a right to access provision may be part of transparency requirements, such as when these provisions require an organization to confirm whether it has data about a specific individual, as well as additional information about the type of information collected, the policies governing that data collection, and what other entities the organization has shared the data with.

GDPR, APEC, OECD, HIPAA, FERPA, CCPA, and CPBR each require some form of right of access.

Table 11: Right-of-access components

Framework	Right-of-Access Components
GDPR	Controllers must provide any information relating to processing to the data subject in a concise, transparent, and easily accessible form, using clear language. This right has a few exceptions, such as for public safety and intellectual property.*
APEC	Individuals should be able to obtain from the personal information controller confirmation of whether the personal information controller holds personal information about them, in a reasonable time for a reasonable expense.
OECD	Individuals have the right to obtain from a data controller confirmation of whether the controller has data relating to them in an intelligible form.†
HIPAA	Individuals have the right to access their health information, with a few exceptions.‡
GLBA	None
FERPA	Parents or eligible students have the right to inspect and review education records maintained by the educational institution or agency, with few exceptions.§
CCPA	A business that receives a verifiable request from a consumer to access personal information shall promptly take steps to disclose and deliver, free of charge, the personal information required by this section.‖
CPBR	Each covered entity shall, upon the request of an individual, provide that individual with reasonable access to, or an accurate representation of, personal data that both pertains to such individual and is under the control of such covered entity.#

*** There are several exceptions, including that access rights not adversely affect the rights or freedoms of others, especially trade secrets or intellectual property protections.[104]**

† Exceptions include by consent of data subject or authority of law.

‡ Exceptions include psychotherapy notes, information compiled in reasonable anticipation of a civil, criminal, or administrative action or proceeding, and more.

§ There are a few exceptions, such as if the education records of a student also containing information about a different student.[105]

‖ This component does not require companies to store data for one-time transactions.[106]

 # There are a few exceptions, such as when access by the individual is limited by applicable law or legally recognized privilege, or any applicable First Amendment interest of the covered entity in that personal data.[107]

Impact

The right of access has clear benefits for consumers because it allows users with strong privacy preferences to make more informed choices. However, the cost of providing data access can be substantial, especially for large, old, and complex data sets, and data sets that are not digitized (e.g., stored on paper in filing cabinets), so the usefulness of this requirement depends on the data in question.

Recommendation

Federal privacy legislation should include a limited right of access for sensitive personal data. This right should require data controllers to disclose whether they have data about a specific individual, the type of information collected, the policies governing that data collection, and with what other entities the organization has shared the data. This right should not apply to proprietary data, which is data about an individual that is inferred or computed by an organization. For example, companies construct online advertising profiles for consumers based on many different sources of observed personal information, such as direct-mail responses, search history, and demographic information. For critical services, data subjects should be able to access this data at no cost. For example, patients should continue to be able to get access to their medical records at no cost, and consumers should have access to their utility usage data. For noncritical services, the law should allow organizations to recover reasonable costs to comply with requests from data subjects. For noncritical services using nonsensitive information (e.g., signing into a building), there should be no requirement to provide access.

12. Data Portability

Data portability is a specific type of right of access that requires organizations to provide consumers a copy of their data in a machine-readable format. The 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. Regarding data portability, only GDPR and HIPAA have specific language that guarantees data subjects have a data portability right.

Table 12: Data-portability components

Framework	Data-Portability Components
GDPR	Individuals have the right to require companies to transmit their personal data to other companies.*
APEC	None
OECD	None
HIPAA	Access rights enable individuals to direct the covered entity to transmit a copy to a designated person or entity of their choice.†
GLBA	None
FERPA	None
CCPA	None
CPBR	None

*** There are several exceptions, including the right to not adversely affect the rights or freedoms of others.[108]**

† Exceptions include psychotherapy notes, information compiled in reasonable anticipation of a civil, criminal, or administrative action or proceeding, and more.[109]

Impact

Data portability has clear benefits for consumers in many cases because it encourages data reuse and promotes competition. For example, it reduces the opportunity for companies to artificially lock in customers by making it too difficult to move their data to another company, and instead encourages companies to retain customers by offering the most valuable services. This sort of anticompetitive behavior has occurred in the real estate, financial services, and air travel industries, where businesses have taken steps to limit third-party access to users' data.[110] Just like access requirements, however, the cost of providing portable data to consumers can be substantial, especially for large, old, complex, and non-digitized data sets. Therefore, the usefulness of data portability also depends on the data in question.

Recommendation

Federal privacy legislation should include data portability for sensitive personal data consumers provide to organizations. These rights should not apply to proprietary data computed by an organization. For critical services, data subjects should be able to access this right at no cost, enabling them to port their data to any third party they choose. For noncritical services, the law should allow organizations to recover reasonable costs to comply with data portability requests from data subjects. Policymakers should be careful to not roll back existing data portability rights in areas such as health care and utilities. There should be no rights to data portability for nonsensitive information used in noncritical services (e.g., the specific flights a person takes in a particular year from a particular airline).

13. Right to Rectification

The right to rectification allows individuals to request that organizations correct information that is inaccurate. Several laws and proposed laws, including HIPAA, FERPA, GDPR, CPBR, OECD, and APEC contain a right to rectification.

Table 13: Right-to-rectification components

Framework	Rectification Components	Exceptions
GDPR	Data subjects have the right to obtain from the covered entity without undue delay the rectification of inaccurate personal data.	Data obtained for purposes related to the public interest, scientific or historical research, or statistical purposes.*
APEC	Data subjects may challenge the accuracy of information relating to them and, if possible and as appropriate, have the information corrected, completed, amended, or deleted.	The burden of rectification is unreasonable, the information should not be disclosed for legal or security reasons, or the privacy of the individual would be violated.
OECD	Data subjects have the right to challenge the use of their data and, if the challenge is successful, have that data erased, corrected, completed, or amended.	None
HIPAA	Does not require covered entities to remove erroneous information, although patients may request to have their records amended.	Covered entities must choose whether to amend records within 60 days.
GLBA	None	N/A
FERPA	Data subjects (or for minors, the parents) have the right to request corrections to records they believe to be inaccurate or misleading.	Covered entities may choose not to amend these records; and there is an appeal process.
CCPA	None	N/A
CPBR	Covered entities provide individuals with means to dispute and resolve, within a reasonable time period, the accuracy or completeness of their personal data.	Whenever requests are incompatible with a legal obligation or First Amendment interest of the covered entity, as well as the enumerated exceptions.†

*** GDPR's principles also do not apply to data rendered anonymous.**

† "Enumerated exceptions" means: preventing fraud; preventing child exploitation or serious violent crime; cybersecurity concerns; protecting the rights or property of the covered entity or, upon consent of the customer, the covered entity's customer; monitoring or enforcing agreements between covered entity and individual; processing customary business; or complying with a legal requirement or governmental request.[111]

Impact

Right to rectification provides important consumer protections in certain cases. For example, allowing users to correct errors in their credit histories can help them avoid harms that would result from erroneous credit information. However, the right to rectification imposes costs on organizations, and when the information is not being used to make important decisions, the cost of correcting trivial errors may be unnecessarily burdensome.

Recommendation

Federal privacy legislation should uphold a limited right to rectification for sensitive data collected by covered entities providing critical services, such as financial and health data. This provision should ensure data remains accurate, such as by requiring evidence for changes to sensitive data sets, like an individual's medical history. However, federal privacy law should not create a broad right to rectification, especially for proprietary data computed or inferred by an organization.

14. Right to Deletion and Right to be Forgotten

The right to deletion requires data controllers to, upon 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.

The right to be forgotten requires search engines to delete, upon request, links to certain personal information published publicly on other websites.[112] GDPR, CCPA, OECD, and CPBR have right to deletion or right to be forgotten provisions.

Table 14: Right to deletion and right to be forgotten

Framework	Right to Deletion and Right to be Forgotten	Exceptions
GDPR	Data subjects have the right to obtain from the controller the irrevocable deletion of their personal data without undue delay, and the controller shall have the obligation to erase personal data without undue delay.	Maintaining information for public safety or a task carried out in the public interest; exercising the right of freedom of expression and information; legal compliance; the performance of a task carried out in the public interest; on the grounds of public interest in the area of public health; for archiving purposes in the public interest; scientific or historical research or statistical purposes; or for the establishment, exercise, or defense of legal claims.*
APEC	None	N/A
OECD	Data subjects have the right to challenge data and, if the challenge is successful, to have the data erased, corrected, completed, or amended.	None
HIPAA	None	N/A
GLBA	None	N/A
FERPA	None	N/A
CCPA	A consumer shall have the right to that a business delete any personal information about the consumer which the business has collected from the consumer.	Maintaining the information being necessary to complete a transaction, providing goods or services requested by the consumer; performing a contract with the consumer; detecting security incidents, fraud, or illegal activity; exercising the right to freedom of speech; complying with other California privacy laws; conducting peer-reviewed scientific, historical, or statistical research; complying with legal obligations; using consumer information internally in a lawful way; and more.
CPBR	If the covered entity declines to correct or amend the personal data, the covered entity shall, upon request and authentication of the person making the request, destroy or delete the personal data the covered entity maintains within a reasonable period of time (45 days), unless the data is exempt.	The covered entity having to comply with a legal obligation or if there is any applicable First Amendment interest of the covered entity; and if deleting that data is for purposes outlined in the enumerated exceptions.†

*** GDPR's principles also do not apply to data rendered anonymous.**

† "Enumerated exceptions" means: preventing fraud; preventing child exploitation or serious violent crime; cybersecurity concerns; protecting the rights or property of the covered entity or, upon consent of the customer, the covered entity's customer; monitoring or enforcing agreements between covered entity and individual; processing customary business; or complying with a legal requirement or governmental request.[113]

Impact

These deletion rights give consumers the ability to require an organization to remove information about them, such as when they decide they no longer want to use a service. These rights can encourage companies to be responsive to consumer needs because consumers can withdraw their consent to data processing at any time. However, the costs of complying with this requirement can mount quickly, especially because a lot of data may be in backups or offline— so applying this rule broadly can impose significant costs.

Some applications of deletion rights, particularly the so-called "right to be forgotten," negatively impact freedom of speech and right to know. Deletion rights can also negatively impact the development of technologies, such as artificial intelligence (AI). Many AI systems develop their decision models by learning from large data sets, and allowing users to permanently delete certain data can render the systems less accurate or even break them entirely.[114]

Recommendation

Federal privacy legislation should not create a right to deletion or a right to be forgotten.

15. Data Retention

Data retention limitations require organizations to delete data after a set period of time. Both GDPR and CPBR have data retention limitations.

Table 15: Data-retention

Framework	Data Retention Limitations	Exceptions
GDPR	Requires covered entities to provide individuals with applicable retention periods and the criteria to determine such periods. Moreover, GDPR requires storage periods to be at a "strict minimum."	Exercising the right of freedom of expression and information; legal compliance; the performance of a task carried out in the public interest; on the grounds of public interest in the area of public health; archiving purposes in the public interest; scientific or historical research or statistical purposes; or for the establishment, exercise, or defense of legal claims.*
APEC	None	N/A
OECD	None	N/A
HIPAA	None	N/A
GLBA	None	N/A
FERPA	None	N/A
CCPA	None	N/A
CPBR	Covered entities must delete, destroy, or de-identify personal data within a reasonable time after it has fulfilled the purpose or purposes for which such personal data was first collected.	There are several enumerated exceptions.†

*** GDPR's principles also do not apply to data rendered anonymous in such a way the data subject is not identifiable.**

† In addition to the enumerated exceptions (listed above), covered entities are exempt when transparency and individual controls satisfy their privacy risk management, or when performing an analysis under the supervision of a Privacy Review Board.[115]

Impact

Data retention limitations reduce the amount of usable data available to organizations. One rationale for data retention limitations is that it limits the potential privacy risks for individuals because there is less data that can be misused or exposed in a data breach. However, these restrictions come at a steep price because they limit organizations from retaining historical data for new and interesting purposes that may ultimately benefits consumers. For example, Pinterest uses historical data to both understand large-scale trends in its service and develop new product ideas.[116] Moreover, data retention limits are inappropriate in many contexts, such as health care or financial services, where old records may still be highly relevant.

Recommendation

Federal privacy legislation should not include data retention limitations.

16. Data Transfers to Other Countries

Restrictions on data transfers to other countries require organizations to either keep data domestically or in certain preapproved countries. Different privacy laws have different data localization requirements.[117] OECD and APEC call for international cooperation in support of data flows and removing barriers to them, whereas GDPR imposes a general prohibition on transfers of EU personal data to foreign countries that have not been predetermined to provide adequate protections that ensure equal protection abroad.[118]

Table 16: Restrictions on the international transfers of data

Framework	Data Transfers to Other Countries
GDPR	Covered entities may transfer personal data to a third country or an international organization only after the controller has provided appropriate safeguards, and when enforceable rights and effective legal remedies for data subjects are available.
APEC	Member countries should take all reasonable and appropriate steps to identify and remove unnecessary barriers to information flows and avoid the creation of any such barriers.
OECD	Member countries should work toward the development of principles—both domestic and international—that will govern the laws applicable to transborder flows of personal data.
HIPAA	None
GLBA	None
FERPA	None
CCPA	None
CPBR	None

Impact

Data is an important input for most industries, not just information industries.[119] Despite the significant benefits to companies, consumers, and national economies that arise from the ability of organizations to easily share data across borders, many countries have erected barriers to cross-border data flows.[120] For example, GDPR unnecessarily restricts data flows from the European Union, and thereby impacts digital trade. Unfortunately, many justify these restrictions on the grounds of privacy and security concerns. However, the notion that data needs to be located domestically to ensure it is secure and private is false. The security of data depends on the measures used to secure it—and consumers and businesses can rely on contracts or laws to limit voluntary data disclosures so data stored abroad receives the same level of protection as data stored locally.[121]

Limiting where organizations can store data imposes a number of costs.[122] Companies must often spend more on IT services and pay for duplicate IT services. At the firm level, barriers to data flows make firms less competitive, as companies will by definition be forced to spend more than necessary on IT services. Such barriers also prevent companies from transferring data that is needed for day-to-day activities, which means companies may have to pay for duplicative services.

Recommendation

Federal privacy legislation should place no limits on cross-border data flows, and ensure data controllers remain liable for the use of their data regardless of where it is stored or processed. They can do so through extraterritorial enforcement mechanisms discussed later in this report.

17. Incentives and Penalties to Sharing Data

Many organizations encourage data sharing. For example, some companies offer consumers incentives to share their personal data, such as discounts on products or services. Those who want to end the practice deride these "pay-for-privacy" offers.[123] Conversely, some businesses deny users access to a service unless they consent to the collection and use of personal information, or charge them more for access.

Privacy laws can prohibit either incentives or penalties for data sharing. Both GDPR and CCPA have these types of provisions.

Table 17: Incentives and user penalties to sharing data

Framework	Incentives and User Penalties to Sharing Data
GDPR	Mandates consent be "freely given" for data sharing in exchange for a service.*
APEC	None
OECD	None
HIPAA	None
GLBA	None
FERPA	None
CCPA	Prohibits businesses from denying goods and services or offering a different level of quality of service when users exercise their rights under the law.†
CPBR	None

*** It is still an open question of whether requiring consent to use a service meets the "freely given" standard.[124]**

† The law does allow certain covered entities to offer different prices, rates, levels, or quality of goods and services to users if that difference is directly related to the value of the user's data.[125] Covered entities can only offer this incentive program if they give users prior opt-in consent for the program and allow them to opt out at any time.[126] Moreover, CCPA forbids using this practice in an unjust, unreasonable, coercive, or usurious way.[127]

Impact

Privacy laws that restrict businesses from offering discounts to customers who share their data, including for targeted advertising, hurt both users and companies. Companies benefit from these relationships by monetizing data through advertising and realizing lower customer acquisition costs. Consumers get direct benefits through lower prices and more customized offerings. Society also benefits from greater levels of efficiency in advertising with less money spent on poorly targeted ads.

Moreover, by restricting companies from limiting services or increasing prices for consumers who opt-out of sharing personal data, these frameworks enable free riders—individuals that opt out but still expect the same services and price—and undercut access to free content and services. This type of rule tries to compensate for regulations that drastically reduce the effectiveness of an important source of income for digital media companies—online advertising—by forcing businesses to offer services even though they cannot effectively generate revenue from users. Online advertising is most effective when advertisers can serve relevant ads. Targeted ads based on information about a user (e.g., browsing history) help deliver higher-value ads. If

regulations reduce the effectiveness of targeted ads, websites— especially those offering free services—will get less revenue.[128] In effect, by enabling users to access online services without providing the information necessary for companies to monetize those services, these provisions create a free-rider problem for online services.

Reducing the effectiveness of advertising may result in some companies, particularly those with thin margins, switching to a fee-for-service or subscription business model, wherein customers would have to pay for services that used to be free.[129] While this change would mean slightly lower living standards for everyone who switches, many low- and middle-income individuals would simply lose access to beneficial services they would not wish to pay for or could no longer afford. Moreover, because a subscription-based model would result in reduced revenues, it would also likely decrease the quality, breadth, and variety of content.

Recommendation

Federal privacy legislation should allow companies to provide incentives for data sharing and not implement policies that prohibit covered entities from penalizing users that do not consent to data sharing.

18. Privacy by Design

Privacy-by-design requires any action a company undertakes that involves processing personal data to be done with data protection and privacy in mind at every step. Only one piece of legislation or framework reviewed in this report adheres to privacy-by-design principles: GDPR. In Article 25, GDPR states that data protection must be developed by design and by default.

Table 18: Privacy by design

Framework	Privacy-by-Design Requirements
GDPR	Requires covered entities to implement appropriate technical and organizational measures in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of GDPR and protect the rights of data subjects.*
APEC	None
OECD	None
HIPAA	None
GLBA	None
FERPA	None
CCPA	None
CPBR	None

Impact

Focusing on privacy at the beginning of a product's life cycle does not always make sense. For example, given that roughly 75 percent of venture-backed start-ups fail, why should these businesses spend time and resources designing privacy into products or services that will not succeed?[130] Moreover, privacy is one of many design objectives for businesses—for example, others are usability, security, and environmental-friendliness—and businesses are best suited to determine when to prioritize different features.

Recommendations

Federal privacy legislation should not include privacy-by-design requirements.

19. Privacy Personnel

Some laws require organizations to designate a specific person be responsible for compliance. Of the laws and frameworks reviewed in this report, GDPR, HIPAA, and GLBA mandate data controllers and processors hire data protection officers.

Table 19: Privacy-personnel requirements

Framework	Privacy Personnel
GDPR	Covered entities must designate a data protection officer if processing is carried out by a public authority (except courts); the core activities of the covered entity consist of processing operations that require regular and systematic monitoring of data subjects on a large scale; or the core activities of the covered entity consist of processing large-scale special categories of data, such as information related to racial or ethnic origin, political opinions, and criminal convictions.*
APEC	None
OECD	None
HIPAA	Requires companies to designate employees to be responsible for the covered entity's mandated information security and privacy programs.
GLBA	Requires companies to designate employees to be responsible for the covered entity's mandated information security and privacy programs.
FERPA	None
CCPA	None
CPBR	None

*** There are many special categories of personal data in GDPR.**[131]

Impact

Personnel requirements force companies to devote excessive resources to compliance, which reduces the amount of money that can be invested in products and services. Indeed, a 2016 study found that GDPR requirements could lead to an additional 75,000 jobs for privacy professionals—a significant expense for organizations.[132] This is a burden particularly for start-ups that have limited resources.

Recommendations

Federal privacy legislation should not require a data protection officer. Instead, legislation should require organizations to provide a means to contact the organization for privacy- and security-related concerns. Firms can then be flexible in their staffing and compliance decisions.

20. Data Security Program

Data security programs specify certain requirements for how organizations protect personal data, without mandating specific technical requirements. This can take two forms. Some laws, such as GDPR and HIPAA, require firms to have a security program of some kind. Other laws, such as GLBA, only disclose their policies and practices related to securing information.

Table 20: Data security programs

Framework	Data-Security-Program Requirements
GDPR	Covered entities must implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk; the ongoing confidentiality, integrity, availability, and resilience of processing systems and services; the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; a process for regularly testing; and the assessment of the effectiveness of technical and organizational measures for ensuring security.
APEC	Covered entities should protect personal information they hold with appropriate safeguards against risks or unauthorized destruction, use, modification, or disclosure of information or other misuses.
OECD	Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure of data.
HIPAA	Covered entities must ensure the confidentiality, integrity, and availability of all electronic protected health information it creates, receives, maintains, or transmits; protecting it against any reasonably anticipated threats or hazards to the security or integrity of such information and against any reasonably anticipated uses or disclosures of such information that are not permitted. It also must ensure compliance by its workforce.
GLBA	Only requires disclosure of security practices.
FERPA	None
CCPA	None
CPBR	Covered entities must identify reasonably foreseeable internal and external risks to the privacy and security of personal data that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information; establish, implement, and maintain safeguards reasonably designed to ensure the security of such personal data; regularly assess the sufficiency of any safeguards in place to control reasonably foreseeable internal and external risks; and evaluate and adjust safeguards in light of the assessment, material changes in operations, or other circumstances that create a material impact on the privacy or security of personal data.

Impact

Data security program requirements can be costly and ineffective. For example, although HIPAA has a data security program requirement, there were 2,181 data breaches involving more than 500 health records between 2009 and 2017.[133] The problem with these requirements is compliance does not necessarily lead to better security. Organizations that make poor decisions about information security may continue to do so, and organizations that are already taking security seriously are not helped by additional compliance obligations.

Recommendations

Federal privacy legislation should not specify the means by which companies protect information, but instead should require them to disclose certain details about their security practices.[134] When companies are more transparent about these practices, consumers can make more informed decisions. If companies suffer from security breaches and these failures are either intentional or result in actual harm to consumers, then regulators like the FTC could take swift enforcement action.

21. Data Breach Notification

Data breach notification requires organizations to notify individuals or regulators when their personal information has been exposed. The goal of notification is to give affected individuals the opportunity to take actions to protect themselves against identity theft or fraud as well as create market pressures on companies to improve their information security practices. Some privacy laws attempt to mitigate breaches after they have occurred by requiring organizations to notify victims. Of the frameworks discussed herein, HIPAA and GDPR have data breach notification components.

Table 21: Data-breach-notification requirements

Framework	Data Breach Notification	Exceptions
GDPR	When personal data breaches are likely to result in a high risk to the rights and freedoms of natural persons, covered entities must communicate the personal data breaches to the data subjects without undue delay.	Personal information being protected through technical or organizational means that render it unintelligible, such as encryption; the risks from disclosure of the data no longer being likely to materialize; and if it involves a disproportionate effort for individual notifications (and a public communication is used instead).
APEC	None	N/A
OECD	None	N/A
HIPAA	A covered entity must, following the discovery of a breach of unsecured protected health information, notify everyone whose unsecured protected health information has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed because of the breach, within 60 days.	Criminal or national security investigations.
GLBA	None	N/A
FERPA	None	N/A
CCPA	None	N/A
CPBR	None*	N/A

*** CPBR includes a provision that says nothing if the bill preempts state data breach laws. However, this bill does not actually propose a standard.**

Impact

Notifying consumers of a data breach if there is a high likelihood of harm enables them to take steps to protect themselves from economic harm. Unfortunately, in the United States, the lack of a uniform federal standard for data breach notification has created both a siloed market where not all users are covered and an unnecessarily complex situation for companies, which must now spend more time navigating this murky legal terrain than protecting consumer data.[135]

Recommendations

Federal privacy legislation should create a single data breach notification standard for all users while simplifying compliance by preempting any conflicting laws from states. In addition, this standard should include data misuse by third parties under certain circumstances.[136] These rules should include a harm analysis provision to determine whether a given data breach or misuse was incidental and would not likely lead to consumer harm. If the breach was not likely to lead to consumer harm, federal privacy legislation should not require consumers be directly notified, but rather only the relevant regulators. This harm standard would help reduce the risk of "data breach fatigue," wherein consumers ignore breach notice warnings simply because they receive so many of them.

22. Data Minimization

Data minimization requires an organization to collect no more data than is necessary to meet specific needs. GDPR, CCPA, CPBR, OECD, and APEC require data minimization.

Table 22: Data minimization

Framework	Data-Minimization Components	Exceptions
GDPR	Covered entities can only hold and process the data absolutely necessary for the completion of their duties, as well as limiting the access to personal data to those needing to act out the processing.	None*
APEC	Covered entities must limit collection to information that is relevant to the purposes of collection, and any such information should be obtained by lawful and fair means, where appropriate, with notice or consent of the individual.	Those uses related to national sovereignty, national security, public safety, and public policy.
OECD	There should be limits to the collection of personal data, and any such data should be obtained by lawful and fair means, where appropriate, with the knowledge or consent of the data subject.	None
HIPAA	None	N/A
GLBA	None	N/A
FERPA	None	N/A
CCPA	Covered entities shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section.	None
CPBR	Each covered entity may only collect, retain, and use personal data in a manner that is reasonable in light of context. Covered entities must also consider ways to minimize privacy risk when determining their personal data collection, retention, and use practices.	There are several enumerated exceptions.†

*** Notably, this principle still applies to data gathered for purposes related to the public interest, scientific or historical research, or statistical purposes.**

† "Enumerated exceptions" means: preventing fraud; preventing child exploitation or serious violent crime; cybersecurity concerns; protecting the rights or property of the covered entity or, upon consent of the customer, the covered entity's customer; monitoring or enforcing agreements between covered entity and individual; processing customary business; or complying with a legal requirement or governmental request.[137]

Impact

Data minimization limits organizations from collecting more data than they need for specific tasks (e.g., mailing a package to someone or processing a payment). Some critics favor data minimization because it fundamentally limits the amount of personal data organizations can collect and therefore reduces privacy risk. Companies that do not have extensive data sources may support this provision, as it reduces the advantage competitors with more data have.

However, this restriction significantly limits companies from exploring new data sets that may lead to new or improved products and services. Data minimization negatively impacts start-ups that, at the outset, do not know what data will be most valuable. 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 these organizations use this data in a way that protects individual privacy. And it impacts businesses' future flexibility by limiting those that want to pivot to different business models based on data. Mandating data minimization can also preclude opportunities to protect individual privacy through de-identification, which can protect sensitive information without unnecessarily sacrificing its value.[138]

Recommendation

Federal privacy legislation should not include data minimization provisions. Organizations should not be discouraged from collecting and using data.

23. Purpose Specification

Purpose limitation restricts companies from using data they have already collected for anything other than the originally stated purpose. HIPAA, GDPR, CCPA, CPBR, OECD, and APEC all have purpose specification requirements.

Table 23: Purpose specification

Framework	Purpose-Specification Component	Exceptions
GDPR	Personal data must be collected for specified, explicit, and legitimate purposes—and not further processed in a manner that is incompatible with those purposes.	Purposes in the public interest, scientific or historical research, and statistical purposes.*
APEC	Personal information collected should be used only to fulfill the purposes of collection and other compatible or related purposes.	Consent of individuals or when necessary to provide a service; and uses relating to national sovereignty, national security, public safety, and public policy.
OECD	The purposes for which personal data is collected should be specified at the time of data collection, and the subsequent use limited to those purposes, or others that are not incompatible with those purposes.	Consent of data subject or authority of law.
HIPAA	A covered entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.	Does not apply to disclosures for treatment, to the individual, or required by law or compliance.
GLBA	None	N/A
FERPA	None	N/A
CCPA	The consumer can request information regarding the purposes for collecting or selling information. A covered entity cannot use personal information collected for additional purposes without providing the consumer with notice.	None
CPBR	Each covered entity may only collect, retain, and use personal data in a manner that is reasonable in light of context. A covered entity shall consider ways to minimize privacy risk when determining its personal data collection, retention, and use practices.	There are several enumerated exceptions.†

*** GDPR's principles also do not apply to data rendered anonymous.**

† "Enumerated exceptions" means: preventing fraud; preventing child exploitation or serious violent crime; cybersecurity concerns; protecting the rights or property of the covered entity or, upon consent of the customer, the covered entity's customer; monitoring or enforcing agreements between covered entity and individual; processing customary business; or complying with a legal requirement or governmental request.[139]

Impact

Purpose specification requires organizations to disclose how they will use data before they collect it, and to use it for that purpose only. This requirement limits organizations from reusing data for new purposes—and by definition, limits innovation. Organizations that rely on data analytics face heightened challenges from purpose specification requirements. It is often not possible to anticipate the insights analytics might reveal from a large data set, and applications of the data set may only become apparent over time. Similarly, under these restrictions, each time medical researchers reuse data or do follow-up studies, they must obtain consent from each patient in the original study—many of whom may have moved, died, or misplaced the researchers' correspondence.[140]

Recommendation

Federal privacy legislation should not include purpose specification. Organizations should be encouraged to discover innovative uses for data.

24. Jurisdiction

Data protection laws can apply in different ways to organizations operating within a country's jurisdiction. Some laws apply to a specific territory, such as by applying to all firms with a physical presence within a particular jurisdiction. For example, a state's privacy law might only apply to businesses with a brick-and-mortar store and business license in that state. Others apply to all firms, including foreign firms, with a domestic impact. A country could create a privacy law that only affects businesses selling products or services to domestic customers or targeting ads domestically. Still others may apply to all firms, including foreign firms, who collect, process, or store data of citizens and residents of a country. GDPR, for instance, applies to all organizations processing data about EU citizens, regardless of where the organizations are physically located or store the data.[141]

Methods of enforcement vary based on jurisdiction. Governments can directly enforce laws that apply to either domestic companies or those with a significant domestic presence. Governments can indirectly enforce laws through agreements with other countries, such as the EU-US Privacy Shield, which authorizes the Federal Trade Commission to take action against companies that violate EU privacy laws.[142]

Table 24: Jurisdiction and extraterritorial enforcement

Framework	Jurisdiction	Extraterritorial Enforcement?
GDPR	European Union	Yes
APEC	APEC Members	N/A*
OECD	OECD Members	N/A*
HIPAA	United States	Yes†
GLBA	United States	Yes†
FERPA	United States	Yes‡
CCPA	California	No§
CPBR	United States	Yes

*** The APEC and OECD frameworks do not require any particular level of enforcement, but rather only call for mutual assistance across borders.**

† These laws do not specifically enable extraterritorial enforcement, although enforcement agencies can pursue extraterritorial cases.[143]

‡ FERPA only applies to educational entities that receive federal funding, which are unlikely to be foreign. However, for foreign third-party associates of covered entities, enforcement agencies can pursue cases.

§ CCPA does not claim extraterritorial enforcement. It is unclear whether California will attempt to enforce its rules with overseas or out-of-state entities. However, CCPA only applies to California consumers. California businesses are not obliged to offer the same protections to consumers from outside the state.

Impact

Companies, whether foreign or domestic, are typically bound to a nation's data protection laws if they do business there. Having a legal presence or engaging in significant business activity is usually sufficient to establish a legal nexus that enables countries to enforce their laws. As a result, firms cannot escape

complying with a nation's privacy laws simply by transferring data overseas. Poorly designed rules on jurisdiction can subject organizations to conflicting laws. Moreover, poorly scoped privacy laws can create toothless rules that subject foreign organizations to laws regulators cannot enforce.

Recommendation

Federal privacy legislation should apply to data controllers with a U.S. nexus—such as having offices, employees, bank accounts, physical property, or substantial marketing in the United States. These data controllers that use third-party data processors should be held responsible for any noncompliance of these third parties, regardless of where those third parties are located. Where organizations store data should have no bearing on their data protection obligations.

25. Harm Focus

Privacy laws impose penalties on organizations for noncompliance. However, some privacy laws use consumers experience as a tangible harm from the misuse of their personal data as a key factor in assessing penalties. Harms exist in several forms.[144] Autonomy violations result in harm for consumers when information they consider sensitive becomes public through involuntary means. Discrimination occurs when personal information is used to deny a person access to something, such as employment, housing, loans, and other goods. Finally, economic harm occurs when a consumer suffers a financial loss or damage because of the misuse of their personal information.

HIPAA, CPBR, and APEC all use some sort of harm standard. Others, such as GDPR, do not consider whether consumers experience harm when assessing violations.

Table 25: Harms-based standards

Framework	Harm-Based Standard
GDPR	None
APEC	First principle is preventing harm. The framework stresses that laws, regulations, and enforcement mechanisms should be designed to prevent harm to individuals from the wrongful collection and misuse of personal data.
OECD	None
HIPAA	Harm is considered in civil penalties.
GLBA	None
FERPA	None
CCPA	None
CPBR	This proposed bill had several components, such as an individual control section, that weighed privacy risk when considering whether to perform an action. A component of privacy risk is harm.*

*** "Privacy risk" means the potential for personal data, on its own or when linked to other information about an individual, to cause emotional distress or physical, financial, professional, or other harm to that individual.**

Impact

Privacy laws that lack a harm standard can create disincentives for companies to take steps that minimize consumer harm and misdirect resources that could be better allocated. For example, privacy laws that apply blanket penalties regardless of tangible consumer harm signal to companies that more money should be spent on compliance, even if that compliance does not improve data protection, and less on innovation.[145] For example, creating rules that result in regulators penalizing a company for a small technical violation of a consumer-protection statute that caused little or no harm will likely push that company to spend more resources on lawyers than on improving the privacy and security of the product itself.[146]

Recommendation

Federal privacy legislation should be based on a standard of substantial and tangible consumer harm when assessing penalties. Doing so will help create a system of incentives to promote desirable behavior while discouraging undesirable behavior, and doing so in a way that limits compliance costs and avoids restricting innovation.

26. Oversight

Oversight mechanisms enable regulators to hold companies accountable by checking whether they are following the rules. Without them, covered entities may skirt their responsibilities to secure personal data. Oversight provisions primarily work in two ways. First, many require companies to submit to compliance audits. For example, GDPR requires companies to demonstrate compliance by contributing to audits and inspections by data protection authorities.[147] Second, privacy laws can give regulatory agencies or attorneys general the ability to investigate complaints and violations.

Table 26: Oversight and investigatory powers provisions

Framework	Oversight Provisions	Investigatory Powers
GDPR	Requires the covered entity to demonstrate compliance and contribute to audits, including inspections.	Gives supervisory authorities investigative powers to order covered entities to provide information, investigate in the form of audits, review verifications, notify controller or processor of alleged infringement, obtain access to information necessary to perform these tasks, and obtain access to any premises of controller or processor.*
APEC	The framework states a personal information controller should be accountable for complying with its principles.	N/A
OECD	The framework states a personal information controller should be accountable for complying with its principles.	N/A.
HIPAA	Requires companies to be prepared for compliance audits.	The Department of Health and Human Services (HHS) secretary can investigate complaints whenever a preliminary review of the facts indicates an alleged violation.
GLBA	Requires companies to be prepared for compliance audits.	Empowers federal banking agencies to jointly establish a consumer complaint mechanism that enables investigation of complaints.
FERPA	Requires covered entities to be prepared for compliance audits.	The Department of Education can investigate whenever a parent or eligible student files a complaint.
CCPA	None	The law empowers the California AG to investigate complaints and violations of the act.
CPBR	Covered entities must take appropriate means to ensure compliance, including training personnel, conducting internal or independent evaluations, building appropriate protections into systems, and following its commitments with respect to purpose specification.	Empowers FTC and state attorneys general to investigate and bring penalties for violations of the act.

*** They are also granted corrective powers to issue warnings, reprimands, and demands for controllers and processers to comply with requests related to rights of individuals.**

Impact

Oversight is important to ensure companies keep their promises and do not ignore their responsibilities. However, like any regulation, these accountability efforts should balance cost with benefits. Requiring yearly audits for private-sector entities in the absence of suspected wrongdoing, for example, would only serve to raise their costs without actually increasing protections. Indeed, companies could spend the money going to these audits on improving their products and services.

Recommendation

Federal privacy legislation should not mandate covered entities implement privacy audits. Moreover, it should ensure accountability requirements do not create unnecessary or burdensome compliance costs.

It should also designate the FTC as the primary regulator for consumer privacy enforcement, using its investigatory powers to protect consumers. However, as policymakers rescind certain sector-based rules to enable the framework proposed in this report, they should also ensure sector-specific regulators stay in place to oversee regulatory changes and continue future enforcement. For example, HHS should continue overseeing the privacy requirements of health providers.

27. Rulemaking Authority

Some privacy legislation gives regulators the authority to promulgate regulations for data controllers. Often, legislation only gives regulators broad policy mandates, which agencies use to create more detailed regulations. In the rulemaking process, regulators release a notice that they are seeking public input so they can use real-world data, industry expertise, and public sentiment to guide final rules. Rulemaking authority also enables regulators to keep rules up to date when facts change or to ensure the spirit of the law addresses changing technologies and business models.

Table 27: Rulemaking authority for regulators

Framework	Regulator	Rulemaking Authority
GDPR	Each member state designates an independent public authority that is responsible for enforcing GDPR.	Only gives independent public authorities supervisory authority, but does not say they can create rules.*
APEC	Does not specify	None
OECD	Does not specify	None
HIPAA	HHS	Gives HHS rulemaking authority.
GLBA	CFPB and FTC†	CFPB has rulemaking authority over the privacy portion of GLBA, except for motor vehicle dealers.
FERPA	The U.S. Department of Education	Gives rulemaking authority to the Department of Education.
CCPA	The attorney general of California	The California AG will establish rules and procedures for the CCPA.‡
CPBR	FTC	Gives FTC rulemaking authority regarding privacy review boards.

*** GDPR creates a European Data Protection Board to ensure consistency of rules enforcement.**

† While CFPB has rulemaking authority, the FTC has enforcement authority.[148]

‡ This is not the traditional federal rulemaking process with comment period.

Impact

Enabling agencies to create rules through public comment is important to ensure transparency and the democratic process in setting regulations. The FTC, which is the primary regulator for consumer privacy in the United States, does not have authority to make rules for data privacy, however, it has created de facto law around privacy and security through its enforcement actions and consent decrees—agreements that subject a company to up to 20 years of audits that can result in penalties for future misconduct.[149] Not only is this process opaque and does not allow for substantial public comment, it can create greater barriers for new entrants by subjecting them to costly, cumbersome, and complex de facto rules that entrench established interests.[150]

Recommendation

Privacy legislation should expand the FTC's authority to create rules around privacy. This approach will enable the FTC to establish clear rules through its public processes and act against companies that knowingly violate them. The statute should be very specific in how the FTC can use this rulemaking ability in order to constrain the agency from becoming an activist regulatory agency that can create regulations more stringent than Congress intends. For example, Congress should direct that such rulemakings address only substantial consumer harms that result from data misuse. The FTC should pay attention to harm and intent when using its enforcement authority against companies to avoid creating perverse incentives.[151] Such clearly-defined and scoped criteria will enable the regulator to also better decide penalties.

28. Penalties

Regulators can assess penalties to punish covered entities that violate the law. Penalties can be either civil or criminal, and levied as fines, public notices, consent decrees regarding future behavior, or imprisonment. GDPR, FERPA, CCPA, and CPBR levy fines for infringement, while violations of HIPAA and GLBA can result in both fines and imprisonment.

Table 28: Penalties

Framework	Fines	Punishments
GDPR	For severe violations, fines can be as high as 20 million euros, or up to 4 percent of a company's total global turnover for the preceding fiscal year	Does not include criminal penalties
APEC	Does not specify	N/A
OECD	Does not specify	N/A
HIPAA	Fines can range from $100 to $50,000 per violation, with a maximum annual penalty of $1.5 million.*	Knowingly violating HIPAA can result in imprisonment of up to one year.*
GLBA	A covered entity can be fined up to $100,000 for each violation, which can double in aggravated cases.	Violators can be imprisoned for up to 5 years for knowingly violating GLBA, and up to 10 years in aggravated cases.
FERPA	Does not levy fines, but violations can result in the loss of federal funding for the covered entity	Does not include criminal penalties
CCPA	Holds intentional violations liable up to $7,500 for each	Does not include criminal penalties
CPBR	Can fine covered entities by multiplying the number of days there were violations by $35,000, or by multiplying the number of affected consumers by $5,000.†	Maintains the FTC's ability to create consent decrees, but does not include criminal penalties

*** Penalties can increase due to willful neglect, or if committed under false pretenses, for personal gain, or for malicious reasons.[152]**

† Fines cannot exceed $25 million.[153]

Impact

Penalties should be proportional to the actual harm caused to consumers. Overly punitive penalties can leave consumers worse off.[154] For example, the mere threat of the absurdly steep fines under GDPR has already caused some businesses to shut down their services in Europe.[155] If penalties are too small, however, they are unlikely to deter data misuse by other actors in the future. Under the current rules, the FTC does not possess original fining authority. Before a company can be fined, it must agree to be placed under a consent decree, and then subsequently violate that agreement. The amount of the fine the FTC has the authority to levy is often a de minimis amount of an infringing company's profits.[156]

Certainly, under the current system, when the FTC does bring a complaint against a company, it often gets widespread notice in the media. And that company potentially being subject to relatively burdensome consent decrees does provide a motivation for other companies within an industry to abide by the de facto rules created by the consent decree. This system, however, is less than optimal.

Recommendation

Federal privacy legislation should expand the FTC's authority to fine companies that violate the law in ways that result from intent (or negligence) and that cause material consumer harm. But Congress should make it clear that the FTC should take a deliberative harms-based approach, as overly aggressive fines can have a negative effect on innovation. The FTC should consider harm and intent when assessing penalties—wherein unintentional and harmless actions elicit the smallest penalties, while intentional and harmful actions elicit the largest ones.[157]

Moreover, federal privacy legislation should not enable the FTC to levy criminal penalties for privacy enforcement cases, but should still be able to levy these criminal penalties for related cases of extreme fraud.

29. Privacy Complaints

Privacy laws can designate a public agency that receives and processes privacy complaints. This entity can then investigate these complaints to ensure covered entities abide by the law. GDPR, HIPAA, GLBA, and FERPA each designate an entity to receive and handle privacy complaints.

Table 29: Privacy complaints

Framework	Privacy Complaints
GDPR	Data subjects have the right to lodge a complaint with any supervisory authority in any member state.
APEC	N/A
OECD	N/A
HIPAA	Requires covered entities to offer notice that individuals can file complaints with either the covered entity or the secretary of HHS; HIPAA gives HHS the ability to informally and formally review, process, and investigate individuals' complaints.
GLBA	Gives individuals the right to lodge a complaint with the FTC.*
FERPA	Designates the U.S. Department of Education to review, process, and investigate individuals' complaints.
CCPA	Does not specify when or whether complaints will be reviewed, processed or investigated.
CPBR	Requires covered entities to offer notice with a contact for inquires and complaints concerning that covered entity's data processing; does not require the FTC to process complaints.

*** The FTC has enforcement authority, while CFPB has rulemaking authority.**[158]

Impact

Outlining how and when consumers can lodge their privacy complaints is an important aspect of any privacy law. Not only does it improve enforcement, as regulators can receive tips as to which covered entities are violating the rules, but it also gives users an outlet to voice their concerns.

Recommendation

Federal privacy legislation should establish the FTC as the federal agency in charge of receiving and processing privacy complaints and provide it with the resources necessary to process these complaints. Where appropriate, the FTC would forward complaints to relevant sector-specific regulators, such as HHS, for health privacy violations.

30. Private Right of Action

Privacy laws can enable users to sue a company directly for civil penalties if that company violates the framework. Of the frameworks discussed therein, three address a private right of action: GDPR, CCPA, and CPBR—with CPBR not enabling these lawsuits.

Table 30: Private right of action

Framework	Private Right-of-Action Components
GDPR	The data subject shall have the right to mandate a not-for-profit body, organization, or association which has been properly constituted in accordance with the law of a member state, has statutory objectives that are in the public interest, and is active in the field of protecting data subjects' rights and freedoms with regard to their personal data to lodge the complaint on their behalf, to exercise their rights.
APEC	None
OECD	None
HIPAA	None
GLBA	None
FERPA	None
CCPA	A consumer may bring an action under CCPA only from a business's alleged failure to "implement and maintain reasonable security procedures and practices" that result in a data breach.
CPBR	Specifically states it does not give a private right of action.

Impact

Private right of action substantially increases companies' legal risks. Introducing this amount of legal risk inevitably leads to unnecessary lawsuits, some initiated by plaintiffs' lawyers. For example, a vague Illinois law that allows consumers to sue companies for using facial recognition technology without their permission has resulted in several significant, but largely groundless, class-action lawsuits against tech companies, such as Facebook, Shutterfly, and Snapchat.[159] Lawyers may be happy with this shift, but consumers will ultimately pay the price. If companies must spend money on compliance and legal fees, they cannot invest that money in other areas, such as by lowering prices, offering discounts, or creating new products and services.

Recommendation

Federal privacy legislation should not create a private right of action. This would unnecessarily expose companies to substantial legal risk, forcing them to focus more on compliance and less on designing safe and innovative products and services for consumers.

Conclusion

Federal data privacy law should have multiple goals. It should improve transparency of organizations' privacy practices. It should establish clear privacy rights for consumers. It should address concrete privacy harms, rather than hypothetical ones, by focusing on the misuse of sensitive data. It should boost oversight and enforcement powers of privacy regulators to deter bad actors while also incentivizing businesses to better protect consumer data. It should ensure companies are transparent about their security practices and define the recourses available to consumers in case of a data breach. And it should preempt states from passing their own conflicting privacy laws to ensure companies are not faced with 50 different state laws.

Most importantly, any legislation and resulting regulations should limit their impact on innovation to the smallest possible amount. This means, among other things, reducing unnecessary regulatory costs and avoiding undermining important uses of data, including online advertising, which supports much of the free content and services on the Internet. And achieving these goals should not come at the expense of other freedoms—such as freedom of choice and freedom of speech—competition, or innovation. Fortunately, establishing data protections and upholding these values are not mutually exclusive. By following the recommendations outlined in this report, policymakers can accomplish these goals.

APPENDIX: RECOMMENDATIONS FOR FEDERAL PRIVACY LEGISLATION

Components	Recommendation
Scope	Scope rules to apply to all types of data.
Preemption	Create a comprehensive federal data privacy law and preempt state and local governments from passing legislation that would add to or diminish from these rules.
Rescission	Rescind existing federal data privacy laws and create a common set of federal protections. Ensure sector-specific regulators stay in place to oversee these changes and continue future enforcement.
Definition of Personal Data	Distinguish between nonsensitive and sensitive personal data.
De-identified Data	Exempt de-identified data.
Publicly Available Data	Exempt publicly available information.
Definition of Covered Entity	Designate a subset of services provided by covered entities as "critical services," which are subject to higher standards and requirements. Do not exempt organizations based on size.
Method of Consent	Require notice for nonsensitive personal data used in noncritical services. Allow opt-out of data collection when organizations provide critical services collecting nonsensitive personal data, or noncritical services collecting sensitive personal data. Require an opt-in standard when organizations provide critical services collecting sensitive personal data.
Non-Consent-Based Data Processing	Create specific, non-consent-based exceptions to the collection and use of both sensitive and nonsensitive personal information.
Transparency	Include transparency requirements and provide consumers with information on what types of organizations can access personal data and how it is being used.
Right of Access	Include a limited right of access that accounts for costs.
Data Portability	Include a limited right to data portability that accounts for costs.
Right to Rectification	Include a limited right to rectification for sensitive data collected by critical services.
Right to Deletion and Right to be Forgotten	Do not include a right to deletion or a right to be forgotten.
Data Retention	Do not include limitations on data retention.
Data Transfers to Other Countries	Do not place limits on cross-border data flows.
Incentives and Penalties to Sharing Data	Do not restrict covered entities from having incentive programs or penalizing users who do not consent to data sharing.
Privacy by Design	Do not include privacy-by-design provisions.
Privacy Personnel	Do not include personnel requirements.
Data Security Program	Do not specify how covered entities protect information, but instead require them to disclose certain details about their security practices.

Data Breach Notification	Create a single data breach notification standard for all users while simplifying compliance by preempting any conflicting laws from states.
Data Minimization	Do not include data-minimization provisions.
Purpose Specification	Do not include purpose-specification provisions.
Jurisdiction	Extend protections extraterritorially.
Harm Focus	Focus enforcement on substantial consumer harms, not hypothetical ones.
Oversight	Give FTC jurisdiction over privacy enforcement. Oversight requirements should weigh costs of compliance with benefits.
Rulemaking Authority	Provide FTC with limited rulemaking authority for data privacy.
Penalties	Expand the FTC's authority to fine companies that violate the law, taking a deliberative harms-based approach.
Privacy Complaints	Establish the FTC as the federal agency in charge of receiving and processing privacy complaints, and provide it with the resources necessary to process these complaints.
Private Right of Action	Do not include a private right of action.

ENDNOTES

1. 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), accessed December 12, 2018, http://www2.itif.org/2018-canada-eu-us-ict-development.pdf.
2. Daniel Castro, "Benefits and Limitations of Industry Self-Regulation for Online Behavioral Advertising" (Information Technology and Innovation Foundation, December 2011), accessed December 12, 2018, http://www.itif.org/files/2011-self-regulation-online-behavioral-advertising.pdf.
3. The Federal Trade Commission Act, 15 U.S.C. § 41 (1914).
4. "Europe's History Explains Why it Will Never Produce a Google," *The Economist*, October 13, 2018, accessed December 4, 2018, https://www.economist.com/europe/2018/10/13/europes-history-explains-why-it-will-never-producea-google.
5. Ibid.
6. 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.
7. Alan McQuinn and Daniel Castro, "Why Stronger Privacy Regulations Do Not Spur Increased Internet Use" (Information Technology and Innovation Foundation, July 2018), accessed December 12, 2018, http://www2.itif.org/2018-trust-privacy.pdf.
8. Ibid.
9. Ira C. Magaziner, "Creating a Framework for Global Electronic Commerce" (The Progress and Freedom Foundation, July 1999), accessed December 12, 2018, http://www.pff.org/issues-pubs/futureinsights/fi6.1globaleconomiccommerce.html.
10. See "Legislative History." S. Comm. on Commerce, Science, and Transportation, Online Personal Privacy Act of 2002, S. Rept. 107-240, No. 551 (2002).
11. Online Privacy Protection Act of 1999, S. 809 (1999), 106th Cong. (1999).
12. The Consumer Internet Privacy Enhancement Act, S. 2928 (2000), 106th Cong. (2000).
13. The Online Personal Privacy Act of 2002, S. 2201 (2002), 107th Cong. (2002).
14. The Consumer Internet Privacy Enhancement Act, H.R. 237 (2001), 107th Cong. (2001).
15. The Commercial Privacy Bill of Rights Act, S.799 (2011), 112th Cong. (2011).
16. "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy" (White House, 2012), accessed December 12, 2018, https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf.
17. Brendan Sasso, "Obama's 'Privacy Bill of Rights' Gets bashed From All Sides," *The Atlantic*, February 27, 2015, accessed December 12, 2018 https://www.theatlantic.com/politics/archive/2015/02/obamas-privacy-bill-of-rights-gets-bashed-from-all-sides/456576/.
18. Balancing the Rights of Web Surfers Equally and Responsibly Act, H.R. 2520 (2017), 115th Cong. (2017).
19. The Customer Online Notification for Stopping Edge-provider Network Transgressions Act, S. 2639 (2018), 115th Cong. (2018).
20. Social Media Privacy Protection and Consumer Rights Act, S. 2728 (2018), 115th Cong. (2018).
21. Information Transparency and Personal Data Control Act, H.R. 6864 (2018), 115th Cong. (2018).
22. "Consumer Data Protection Act Discussion Draft," Office of Sen. Ron Wyden, accessed December 12, 2018, https://www.wyden.senate.gov/imo/media/doc/Wyden%20Privacy%20Bill%20one%20pager%20Nov%201.pdf.
23. Data Care Act of 2018, S. 3744 (2018), 115th Cong. (2018).
24. National Telecommunications and Information Administration, "NTIA Seeks Comment on New Approach to Consumer Data Privacy," *press release*, September 25, 2018, accessed December 18, 2018, https://www.ntia.doc.gov/press-release/2018/ntia-seeks-comment-new-approach-consumer-data-privacy.
25. California Consumer Privacy Act, California Civil Code § 1798.100 - § 1798.198 (2018).

26. Daniel Castro, "ITIF Speaks Out Against California Privacy Law, Calls for Federal Privacy Legislation," *Information Technology and Innovation Foundation,* press release, June 29, 2018, accessed December 12, 2018, https://itif.org/publications/2018/06/29/itif-speaks-out-against-california-privacy-law-calls-federal-privacy.

27. Vermont, Act 171 (2018), accessed December 18, 2018, https://legislature.vermont.gov/bill/status/2018/H.764

28. "Privacy Legislation Related to Internet Service Providers – 2018," National Conference of State Legislatures, November 16, 2018, accessed December 18, 2018, http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-legislation-related-to-internet-service-providers-2018.aspx.

29. "Washington Becomes the Third State with a Biometric Law," *Inside Privacy*, May 31, 2017, accessed December 18, 2018, https://www.insideprivacy.com/united-states/state-legislatures/washington-becomes-the-third-state-with-a-biometric-law/.

30. "Current Unmanned Aircraft State Law Landscape," National Conference of State Legislatures, September 10, 2018, accessed December 18, 2018, http://www.ncsl.org/research/transportation/current-unmanned-aircraft-state-law-landscape.aspx.

31. "Privacy Legislation Related to Internet Service Providers – 2018," National Conference of State Legislatures.

32. "Framework for Responsible Data Protection Regulation" (Google, September 2018), accessed December 21, 2018, https://services.google.com/fh/files/blogs/google_framework_responsible_data_protection_regulation.pdf; Kathy Grillo, "Privacy: It's Time for Congress to Do Right By Consumers," *Verizon*, October 9, 2018, accessed December 21, 2018, https://www.verizon.com/about/news/privacy-its-time-congress-do-right-consumers; Rachel Welch, "Examining Safeguards for Consumer Data Privacy Before the Senate Committee on Commerce, Science, and Transportation," (Charter, September 26, 2018), testimony before the U.S. Senate Committee on Commerce, Science, and Transportation, accessed December 21, 2018, https://www.commerce.senate.gov/public/_cache/files/9cb79c7e-815c-4091-80d0-f425105b110b/2C25167C9296C00C1CBBEBD03171F49A.09-24-18welch-testimony.pdf; Business Roundtable, "Business Roundtable Outlines Priorities on Consumer Data Privacy," *press release*, November 9, 2018, accessed December 21, 2018, https://www.businessroundtable.org/business-roundtable-outlines-priorities-on-consumer-data-privacy; "IA Privacy Principles for a Modern National Regulatory Framework" (Internet Association, November 2018), accessed December 21, 2018, https://internetassociation.org/files/ia_privacy-principles-for-a-modern-national-regulatory-framework_full-doc/; "Framework to Advance Interoperable Rules (FAIR) on Privacy" (The Information Technology Industry Council, October 2018), accessed December 21, 2018, https://www.itic.org/public-policy/FINALFrameworktoAdvanceInteroperableRules%28FAIR%29onPrivacyFinal_NoWatermark.pdf; "U.S. Chamber Privacy Principles" (U.S. Chamber of Commerce, September 2018), accessed December 21, 2018, https://www.uschamber.com/sites/default/files/9.6.18_us_chamber_-_ctec_privacy_principles.pdf; India McKinney and Adam Schwartz, "EFF to U.S. Department of Commerce: Protect Consumer Data Privacy," *Electronic Frontier Foundation*, November 12, 2018, accessed December 21, 2018, https://www.eff.org/deeplinks/2018/11/eff-us-department-commerce-protect-consumer-data-privacy; "Creating a Data Protection Framework: a Do's and Don'ts Guide for Lawmakers" (Access Now, January 2018), accessed December 21, 2018, https://www.accessnow.org/cms/assets/uploads/2018/01/Data-Protection-Guilde-for-Lawmakers-Access-Now.pdf; Nuala O'Connor, "Consumer Data Privacy: Examining Lessons From the European Union's General Data Protection Regulation and the California Consumer Privacy Act" (Center for Democracy and Technology, October 10, 2018), testimony before the U.S. Senate Committee on Commerce, Science, and Transportation, accessed December 21, 2018, https://cdt.org/files/2018/10/2018-10-09-FINAL-Nuala-OConnor-Written-Testimony-Senate-Commerce.pdf.

33. Michelle Richardson, "Americans Deserve a Law Protecting Their Digital Privacy – Here's Our Proposal," (Center for Democracy and Technology, December 13, 2018), accessed December 18, 2018, https://cdt.org/blog/americans-deserve-a-law-protecting-their-digital-privacy-heres-our-proposal/.

34. McQuinn and Castro, "Why Stronger Privacy Regulations Do Not Spur Increased Internet Use."

35. Avi Goldfarb and Catherine E. Tucker, "Privacy Regulation and Online Advertising." SSRN Scholarly Paper ID 1600259, 2010, Rochester, NY, Social Science Research Network, accessed December 12, 2018, https://papers.ssrn.com/abstract=1600259.

36. PwC, "GDPR Compliance Top Data Protection Priority for 92% of US Organizations in 2017, According to PwC Survey," news release, January 23, 2017, https://www.pwc.com/us/en/press-releases/2017/pwc-gdpr-compliance-press-release.html.

37. Rita Heimes and Same Pfeifle, “Study: GDPR’s Global Reach to Require at Least 75,000 DPOs Worldwide.” November 9, 2016, accessed December 4, 2018, https://iapp.org/news/a/study-gdprs-globalreach-to-require-at-least75000-dpos-worldwide/.

38. Jessica Davies, “ ‘The Google Data Protection Regulation’: GDPR is strafing ad sellers,” *DigiDay*, June 4, 2018, accessed December 18, 2018, https://digiday.com/media/google-data-protection-regulation-gdpr-strafing-ad-sellers/.

39. “Websites not available in the European Union after GDPR,” VerifiedJoseph.com, July 11, 2018, updated November 16, 2018, accessed December 18, 2018, https://data.verifiedjoseph.com/dataset/websites-not-available-eu-gdpr.

40. Nick Wallace and Daniel Castro, “The Impact of the EU’s New Data Protection Regulation on AI,” (Center for Data Innovation, March 27, 2018), accessed December 4, 2018, http://www2.datainnovation.org/2018-impact-gdpr-ai.pdf.

41. Avi Goldfarb and Catherine Tucker, “Privacy and Innovation” (National Bureau of Economic Research, 2011), http://www.nber.org/papers/w17124; Avi Goldfarb and Catherine E. Tucker, “Privacy Regulation and Online Advertising,” *Management Science* 57, no. 1 (2011), 57–71.

42. James Campbell, Avi Goldfarb, and Catherine Tucker, “Privacy Regulation and Market Structure” (working paper, SSRN, 2011), accessed December 12, 2018, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1729405.

43. L. Christensen, et al., “The Impact of the Data Protection Regulation in the EU” (Intertic, 2013), http://www.intertic.org/new_site/wp-content/uploads/Policy%20Papers/CCER.pdf.

44. Booz and Company, “The Impact of E.U. Internet Privacy Regulations on Early-Stage Investment A Quantitative Study,” accessed December 18, 2018, 18, https://www.strategyand.pwc.com/media/uploads/Strategyand-Impact-EU-Internet-Privacy-Regulations-Early-Stage-Investment.pdf.

45. Anja Lambrecht, “E-Privacy Provisions and Venture Capital Investments in the EU,” (2017), accessed December 18, 2018, https://www.ceps.eu/sites/default/files/E-Privacy%20Provisions%20and%20Venture%20Capital%20Investments%20in%20the%20EU.PDF.

46. PwC, “IAB Internet Advertising Revenue Report 2012 Full Year Results April 2013, https://www.iab.com/wp-content/uploads/2015/05/IABInternetAdvertisingRevenueReportFY2012POSTED.pdf; PwC, “IAB Internet Advertising Revenue Report 2017 Full Year Results, May 2018, accessed December 18, 2018, https://www.iab.com/wp-content/uploads/2018/05/IAB-2017-Full-Year-Internet-Advertising-Revenue-Report.REV2_.pdf; IAB, “The Definitive Guide to the European Digital Advertising Market,” 2017, https://www.iabeurope.eu/wp-content/uploads/2018/06/IAB-Europe_AdEx-Benchmark-2017-Report_FINAL-V2.pdf.

47. HIS Technology, “Paving the Way: How Online Advertising Enables the Digital Economy of the Future,” accessed December 18, 2018, 18, https://www.iabeurope.eu/files/9614/4844/3542/IAB_IHS_Euro_Ad_Macro_FINALpdf.

48. Robert Atkinson, “How ICT Can Restore Lagging European Productivity Growth” (Information Technology and Innovation Foundation, October 2018), accessed December 12, 2018, http://www2.itif.org/2018-ict-eu-productivity-growth.pdf.

49. McQuinn and Castro, “Why Stronger Privacy Regulations Do Not Spur Increased Internet Use.”

50. Daniel Castro and Alan McQuinn, “Comments to the National Telecommunications and Information Administration on its Privacy Request for Comment” (Information Technology and Innovation Foundation, November 8, 2018). Accessed December 12, 2018, 5, http://www2.itif.org/2018-ntia-privacy-comments.pdf.

51. David Redl, “New Data Show Substantial Gains and Evolution in Internet Use,” *National Telecommunications and Information Administration*, June 6, 2018, accessed December 18, 2018, https://www.ntia.doc.gov/blog/2018/new-data-show-substantial-gains-and-evolution-internet-use.

52. Daniel Castro, “Time to Retire Social Security Numbers,” *RealClear Policy*, September 6, 2017, accessed November 13, 2018, https://www.realclearpolicy.com/articles/2017/09/16/time_to_retire_social_security_numbers_110358.html.

53. Daniel Castro, “Bank Privacy Notices Cost Consumers Over $700M Annually,” *Innovation Files*, June 22, 2012, https://www.innovationfiles.org/bank-privacy-notices-costs-consumers-over-700m-annually/.

54. "Designation of the Data Protection Officer," Regulation (EU) 2016/679 (General Data Protection Directive), OJ L 119, March 05, 2016, Articles 37, https://gdpr-info.eu/art-37-gdpr/.

55. The Federal Trade Commission Act, 15 U.S.C. § 41 (1914).

56. Maureen K. Ohlhausen, "Putting the FTC Cop Back on the Beat" (Federal Trade Commission, November 18, 2017), accessed December 12, 2018, https://www.ftc.gov/system/files/documents/public_statements/1280393/putting_the_ftc_cop_back_on_the_beat_mko.pdf.

57. David McCabe, "Mergers are spiking, but antitrust cop funding isn't," *Axios*, May 7, 2018, accessed December 12, 2018, https://www.axios.com/antitrust-doj-ftc-funding-2f69ed8c-b486-4a08-ab57-d3535ae43b52.html.

58. Daniel Castro and Alan McQuinn, "How and When Regulators Should Intervene" (Information Technology and Innovation Foundation, February 2015), http://www2.itif.org/2015-how-whenregulators-intervene.pdf."

59. "Adicionar un Capítulo Terecero al Tíitulo V de la Circular Única," Industria y Comercio Superintendencia, August 10, 2017, accessed December 12, 2018, http://www.sic.gov.co/sites/default/files/normatividad/082017/Circular_Externa_005_de_2017.pdf.

60. Nigel Cory and Alan McQuinn, "Will the US capitalize on its opportunity to stop data localization?" *The Hill*, September 9, 2018, accessed October 19, 2018, https://thehill.com/opinion/cybersecurity/405422-will-the-us-capitalize-on-its-opportunity-to-stop-data-localization.

61. 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; California Consumer Privacy Act, California Civil Code § 1798.100 - § 1798.198 (2018); "Administration Discussion Draft: The Consumer Privacy Bill of Rights of 2015," *Obama White House*, 2015, accessed December 18, 2018, https://obamawhitehouse.archives.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf; "OECD Privacy Principles" (Organisation for Economic Co-operation and Development, 1980), accessed December 20, 2018, http://oecdprivacy.org/; "APEC Privacy Framework" (Asia-Pacific Economic Cooperation, 2015) accessed December 20, 2018.

62. The Health Insurance Portability and Accountability Act of 1996, Pub. L. 104–191, 110 Stat. 1936, (1996); The Gramm-Leach-Bliley Act, the Financial Services Modernization Act of 1999, Pub. L. 106–102, 113 Stat. 1338, (1999); The Family Educational Rights and Privacy Act, § 513 of Pub. L. 93-380, (1974).

63. The Gramm-Leach-Bliley Act, the Financial Services Modernization Act of 1999, Pub. L. 106–102, 113 Stat. 1338, (1999).

64. Regulation (EU) 2016/679 (General Data Protection Directive).

65. The Health Insurance Portability and Accountability Act of 1996, Pub. L. 104–191, 110 Stat. 1936, (1996); The Family Educational Rights and Privacy Act, § 513 of Pub. L. 93-380, (1974).

66. "Security Breach Notification Laws," National Conference of State Legislatures, September 29, 2018, accessed December 18, 2018, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

67. Daniel Castro and Alan McQuinn, "Why We need a Robust National Standard For Data Breach Notification," *The Christian Science Monitor*, June 10, 2015, accessed December 12, 2018, https://www.csmonitor.com/World/Passcode/Passcode-Voices/2015/0610/Opinion-Why-we-need-a-robust-national-standard-for-data-breach-notification.

68. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) http://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN.

69. The Health Insurance Portability and Accountability Act of 1996, Pub. L. 104–191, 110 Stat. 1936, (1996); The Family Educational Rights and Privacy Act, § 513 of Pub. L. 93-380, (1974).

70. The Health Insurance Portability and Accountability Act of 1996, § 160.103.

71. "Administration Discussion Draft: The Consumer Privacy Bill of Rights of 2015," *Obama White House.*

72. Ibid.

73. Robert Atkinson, Daniel Castro and Alan McQuinn, "ITIF Filing to FTC on Informational Injury Workshop" (Information Technology and Innovation Foundation, October 27, 2017), accessed December 12, 2018, https://itif.org/publications/2017/10/27/itif-filing-ftc-informational-injury-workshop.
74. Ann Cavoukian and Daniel Castro, "Big Data and Innovation, Setting the Record Straight: De-identification Does Work" (Information Technology and Innovation Foundation, June 16, 2014), accessed December 12, 2018, http://www2.itif.org/2014- big-data-deidentification.pdf.
75. "OECD Privacy Principles" (Organisation for Economic Co-operation and Development, 1980), accessed December 20, 2018, http://oecdprivacy.org/.
76. "Data Protection By Design and By Default," Regulation (EU) 2016/679 (General Data Protection Directive), Art. 25, https://gdpr-info.eu/art-25-gdpr/.
77. "Processing for Statistical Purposes," Regulation (EU) 2016/679 (General Data Protection Directive), Recital 162, https://gdpr-info.eu/recitals/no-162/.
78. California Consumer Privacy Act, California Civil Code § 1798.140 (S)(2).
79. "Administration Discussion Draft: The Consumer Privacy Bill of Rights of 2015," *Obama White House,* Sec. 4.
80. Cavoukian and Castro, "Big Data and Innovation, Setting the Record Straight: De-identification Does Work."
81. Simson Garfinkle, "De-identification of Personal Information" (National Institute of Science and Technology, October 2015), accessed December 18, 2018, https://nvlpubs.nist.gov/nistpubs/ir/2015/nist.ir.8053.pdf.
82. "Personal Data," Regulation (EU) 2016/679 (General Data Protection Directive), Art. 4, https://gdpr-info.eu/recitals/no-47/.
83. The Health Insurance Portability and Accountability Act of 1996, Pub. L. 104–191, 110 Stat. 1936, (1996); The Health Insurance Portability and Accountability Act of 1996, Pub. L. 104–191.
84. "Administration Discussion Draft: The Consumer Privacy Bill of Rights of 2015," *Obama White House*, 2015, accessed December 18, 2018, https://obamawhitehouse.archives.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf.
85. Daniel Castro, "Data Privacy Principles for Spurring Innovation" (Information Technology and Innovation Foundation, June 2010), accessed December 18, 2018, http://www.itif.org/files/2010-privacy-and-innovation.pdf.
86. The Family Educational Rights and Privacy Act, § 513 of Pub. L. 93-380, (1974).
87. "Overriding Legitimate Interest," Regulation (EU) 2016/679 (General Data Protection Directive), Recital 47, https://gdpr-info.eu/recitals/no-47/.
88. An authorization is a detailed document that gives covered entities permission to use protected health information for specified purposes, which are generally other than treatment, payment, or health-care operations, or to disclose protected health information to a third party specified by the individual. An authorization must specify a number of elements, including a description of the protected health information to be used and disclosed, the person authorized to make the use or disclosure, the person to whom the covered entity may make the disclosure, an expiration date, and, in some cases, the purpose for which the information may be used or disclosed. The Health Insurance Portability and Accountability Act of 1996, Pub. L. 104–191, 110 Stat. 1936, (1996).
89. Alan McQuinn, "The Economics of "Opt-Out" Versus "Opt-In" Privacy Rules," *Information Technology and Innovation Foundation*, October 6, 2017, accessed December 18, 2018, https://itif.org/publications/2017/10/06/economics-opt-out-versus-opt-in-privacy-rules.
90. McQuinn and Castro, "Why Stronger Privacy Regulations Do Not Spur Increased Internet Use."
91. Avi Goldfarb and Catherine E. Tucker, "Privacy Regulation and Online Advertising." SSRN Scholarly Paper ID 1600259, 2010, Rochester, NY, Social Science Research Network, accessed June 12, 2018, https://papers.ssrn.com/abstract=1600259.
92. McQuinn, "The Economics of "Opt-Out" Versus "Opt-In" Privacy Rules."
93. "Consent," Regulation (EU) 2016/679 (General Data Protection Directive), https://gdpr-info.eu/issues/consent/.
94. "Lawfulness of Processing," Regulation (EU) 2016/679 (General Data Protection Directive), Art. 6, https://gdpr-info.eu/art-6-gdpr/.

95. The Family Educational Rights and Privacy Act, §99.30-99.39, (1974).
96. California Consumer Privacy Act, California Civil Code § 1798.185 (2018).
97. Alan McQuinn, "Commentary: E.U. data privacy rules threaten medical research," *FedScoop*, November 18, 2014, accessed December 20, 2018, https://www.fedscoop.com/eu-data-privacy-rules-threaten-derail-medical-research/.
98. Regulation (EU) 2016/679 (General Data Protection Directive), Article 13, https://gdpr-info.eu/art-13-gdpr/.
99. The Health Insurance Portability and Accountability Act of 1996, §164.520.
100. Besides some sector-specific regulations, privacy policies and notices from websites in the United States are mandated by California law, rather than federal law. California Online Privacy Protection Act, California Bus. & Prof. Code § 22575-22578 (2003).
101. This type of enforcement falls under the FTC's unfair and deceptive practices authority. The Federal Trade Commission Act, 15 U.S.C. § 41 (1914).
102. "Privacy Nutrition Labels," Cylab, accessed December 18, 2018, https://cups.cs.cmu.edu/privacyLabel/.
103. Daniel Castro and Alan McQuinn, "The Economic Costs of the European Union's Cookie Notification Policy" (Information Technology and Innovation Foundation, November 2014), accessed December 20, 2018, http://www2.itif.org/2014-economic-costs-eu-cookie.pdf.
104. "Right of Access," Regulation (EU) 2016/679 (General Data Protection Directive), Recital 63, https://gdpr-info.eu/recitals/no-63/.
105. The Family Educational Rights and Privacy Act, §99.10.
106. California Consumer Privacy Act, California Civil Code § 1798.100.
107. "Administration Discussion Draft: The Consumer Privacy Bill of Rights of 2015," *Obama White House*, Sec. 106.
108. "Right to Data Portability," Regulation (EU) 2016/679 (General Data Protection Directive), Art. 20, https://gdpr-info.eu/art-20-gdpr/.
109. The Health Insurance Portability and Accountability Act of 1996, §164.524.
110. Daniel Castro and Michael Steinberg, "Blocked: Why Some Companies Restrict Data Access to Reduce Competition and How Open APIs Can Help" (Center for Data Innovation, November 6, 2017), accessed December 12, 2018, http://www2.datainnovation.org/2017-open-apis.pdf.
111. CPBR outlines several "enumerated exceptions," including: (1) Preventing or detecting fraud; (2) Preventing or detecting child exploitation or serious violent crime; (3) Protecting the security of devices, networks, or facilities; (4) Protecting the rights or property of the covered entity or, upon consent of the customer, the covered entity's customer; (5) Monitoring or enforcing agreements between the covered entity and an individual, including but not limited to, terms of service, terms of use, user agreements, or agreements concerning monitoring criminal activity; (6) Processing customary business records (to the extent that such records are retained for reasonable periods of time or as legally required); or (7) Complying with a legal requirement or responding to an authorized governmental request. "Administration Discussion Draft: The Consumer Privacy Bill of Rights of 2015."
112. Alan McQuinn, "Another Problem with the 'Right to be Forgotten'," *Innovation Files,* August 25, 2014, accessed December 12, 2018, https://www.innovationfiles.org/another-problem-with-the-right-to-be-forgotten/.
113. CPBR outlines several "enumerated exceptions," including: (1) preventing or detecting fraud; (2) preventing or detecting child exploitation or serious violent crime; (3) protecting the security of devices, networks, or facilities; (4) protecting the rights or property of the covered entity or, upon consent of the customer, the covered entity's customer; (5) monitoring or enforcing agreements between the covered entity and an individual, including but not limited to, terms of service, terms of use, user agreements, or agreements concerning monitoring criminal activity; (6) processing customary business records (to the extent that such records are retained for reasonable periods of time or as legally required); or (7) complying with a legal requirement or responding to an authorized governmental request. "Administration Discussion Draft: The Consumer Privacy Bill of Rights of 2015."
114. Wallace and Castro, "The Impact of the EU's New Data Protection Regulation on AI."

115. CPBR creates Privacy Review Boards to provide additional analysis and determine exemptions under the Act, such as if the benefits of a particular analysis outweigh the likely risks. CPBR also outlines several "enumerated exceptions," including: (1) preventing or detecting fraud; (2) preventing or detecting child exploitation or serious violent crime; (3) protecting the security of devices, networks, or facilities; (4) protecting the rights or property of the covered entity or, upon consent of the customer, the covered entity's customer; (5) monitoring or enforcing agreements between the covered entity and an individual, including but not limited to, terms of service, terms of use, user agreements, or agreements concerning monitoring criminal activity; (6) processing customary business records (to the extent that such records are retained for reasonable periods of time or as legally required); or (7) complying with a legal requirement or responding to an authorized governmental request. "Administration Discussion Draft: The Consumer Privacy Bill of Rights of 2015."
116. Joshua New, "5 Q's for Andrea Burbank, Search and Data Mining Engineer at Pinterest," *Center for Data Innovation*, February 23, 2015, accessed December 12, 2018, http://www.datainnovation.org/2015/02/4077/.
117. Stephen J. Ezell, Robert D. Atkinson, and Michelle A. Wein, "Localization Barriers to Trade: Threat to the Global Innovation Economy" (Information Technology and Innovation Foundation, September 2013), accessed December 12, 2018, http://www2.itif.org/2013-localization-barriers-to-trade.pdf.
118. Regulation (EU) 2016/679 (General Data Protection Directive), Recital 101, https://gdpr-info.eu/recitals/no-101/.
119. Daniel Castro and Alan McQuinn, "Cross-Border Data Flows Enable Growth in All Industries" (Information Technology and Innovation Foundation, February 2015), accessed December 12, 2018, http://www2.itif.org/2015-crossborder-data-flows.pdf.
120. Ezell, Atkinson, and Wein, "Localization Barriers to Trade: Threat to the Global Innovation Economy."
121. Daniel Castro, "The False Promise of Data Nationalism" (Information Technology and Innovation Foundation, December 2013), accessed December 12, 2018, http://www2.itif.org/2013-false-promise-data-nationalism.pdf.
122. Nigel Cory. "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?" (Information Technology and Innovation Foundation, May 1, 2017), accessed December 12, 2018, https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost.
123. See discussion of this phenomenon in this ITIF report. Doug Brake, Daniel Castro, and Alan McQuinn, "Broadband Privacy: The Folly of Sector-Specific Rules" (Information Technology and Innovation Foundation, March 2016), accessed December 20, 2018, http://www2.itif.org/2016-broadband-privacy-folly.pdf.
124. Johnny Ryan, "Can websites use "tracking walls" to force consent under GDPR?" PageFair, November 30, 2017, accessed December 18, 2018, https://pagefair.com/blog/2017/tracking-walls/.
125. California Consumer Privacy Act, California Civil Code § 1798.125.
126. Ibid.
127. Ibid.
128. McQuinn and Castro, "Why Stronger Privacy Regulations Do Not Spur Increased Internet Use."
129. Alan McQuinn, "The Detractors are Wrong, Online Ads Add Value," Information Technology and Innovation Foundation, December 8, 2016, accessed December 12, 2018, https://itif.org/publications/2016/12/08/detractors-are-wrong-online-ads-add-value.
130. Faisal Hoque, "Why Most Venture-Backed Companies Fail," *Fast Company*, December 10, 2012, accessed December 18, 2018,https://www.fastcompany.com/3003827/why-most-venture-backed-companies-fail.
131. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited. Regulation (EU) 2016/679 (General Data Protection Directive), Article 9 and 10, https://gdpr-info.eu/art-9-gdpr/; https://gdpr-info.eu/art-10-gdpr/.
132. Rita Heimes and Same Pfeifle, "Study: GDPR's Global Reach to Require at Least 75,000 DPOs Worldwide." November 9, 2016, accessed December 12, 2018. https://iapp.org/news/a/study-gdprs-globalreach-to-require-at-least-75000-dpos-worldwide/.
133. "Healthcare Data Breach Statistics," *HIPAA Journal*, 2018, accessed December 18, 2018, https://www.hipaajournal.com/healthcare-data-breach-statistics/.

134. Daniel Castro, "How Congress Can Fix the Internet of Things Security," *The Hill*, October 28, 2016, accessed December 12, 2018, https://thehill.com/blogs/pundits-blog/technology/303302-how-congress-can-fix-internet-of-things-security.
135. Castro and McQuinn, "Why We need a Robust National Standard For Data Breach Notification."
136. This includes applying the standard to first-party data, implementing harm analyses, and requiring companies to disclose what steps they take to ensure business partners adhere to data handling practices. See, Daniel Castro, "States Should Revisit Their Data Breach Laws," *Government Technology,* June 2018, accessed December 12, 2018, http://www.govtech.com/policy/States-Should-Revisit-Their-Data-Breach-Laws.html.
137. CPBR outlines several "enumerated exceptions," including: (1) preventing or detecting fraud; (2) preventing or detecting child exploitation or serious violent crime; (3) protecting the security of devices, networks, or facilities; (4) protecting the rights or property of the covered entity or, upon consent of the customer, the covered entity's customer; (5) monitoring or enforcing agreements between the covered entity and an individual, including but not limited to, terms of service, terms of use, user agreements, or agreements concerning monitoring criminal activity; (6) processing customary business records (to the extent that such records are retained for reasonable periods of time or as legally required); or (7) complying with a legal requirement or responding to an authorized governmental request. "Administration Discussion Draft: The Consumer Privacy Bill of Rights of 2015."
138. Cavoukian and Castro, "Big Data and Innovation, Setting the Record Straight: De-identification Does Work."
139. CPBR outlines several "enumerated exceptions," including: (1) preventing or detecting fraud; (2) preventing or detecting child exploitation or serious violent crime; (3) protecting the security of devices, networks, or facilities; (4) protecting the rights or property of the covered entity or, upon consent of the customer, the covered entity's customer; (5) monitoring or enforcing agreements between the covered entity and an individual, including but not limited to, terms of service, terms of use, user agreements, or agreements concerning monitoring criminal activity; (6) processing customary business records (to the extent that such records are retained for reasonable periods of time or as legally required); or (7) complying with a legal requirement or responding to an authorized governmental request. "Administration Discussion Draft: The Consumer Privacy Bill of Rights of 2015."
140. Alan McQuinn, "Commentary: E.U. data privacy rules threaten medical research" *FedScoop*, November 18, 2014, accessed July 22, 2018, https://www.fedscoop.com/eu-data-privacy-rules-threaten-derail-medical-research.
141. "Transfers of Personal Data to Third Countries or International Organisations," Regulation (EU) 2016/679 (General Data Protection Directive), Art. 44-50, https://gdpr-info.eu/chapter-5/.
142. COMMISSION IMPLEMENTING DECISION (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, http://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32016D1250&from=EN.
143. For example, see Cogent Healthcare breach with HIPAA. Marianne Kolbasuk McGee, "HIPAA Omnibus and Offshore Vendors," *Healthcare Info Security*, August 14, 2013, https://www.healthcareinfosecurity.com/hipaa-omnibus-offshore-vendors-a-5987.
144. Atkinson, Castro and McQuinn, "ITIF Filing to FTC on Informational Injury Workshop."
145. Castro and McQuinn, "How and When Regulators Should Intervene."
146. Daniel Castro and Alan McQuinn, "Comments to FTC on Nomi Technologies, Inc." (Information Technology and Innovation Foundation, May 26, 2015), accessed December 12, 2018, https://itif.org/publications/2015/05/26/comments-ftc-nomi-technologies-inc.
147. "Processor," Regulation (EU) 2016/679 (General Data Protection Directive), Art. 28, https://gdpr-info.eu/art-28-gdpr/.
148. "Gramm-Leach Bliley Act," (Federal Trade Commission (FTC), https://www.ftc.gov/enforcement/statutes/gramm-leach-bliley-act.
149. Daniel Solove and Woody Hartzog, "The FTC and the New Common Law of Privacy" 114 Columbia L. Rev. 583, (2014), accessed December 12, 2018, https://cyberlaw.stanford.edu/files/publication/files/SSRN-id2312913.pdf.
150. Castro and McQuinn, "How and When Regulators Should Intervene."
151. Ibid.

152. "What are the Penalties for HIPAA Violations?" *HIPAA Journal*, June 24, 2015, accessed December 18, 2018, https://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096/.
153. "Administration Discussion Draft: The Consumer Privacy Bill of Rights of 2015," *Obama White House*, Sec. 203.
154. McQuinn and Daniel Castro, "Why Stronger Privacy Regulations Do Not Spur Increased Internet Use."
155. Daniel Castro and Alan McQuinn, "GDPR Freeloaders: Why Other Countries Should Fight Back," *Information Technology and Innovation Foundation*, August 16, 2018, accessed December 12, 2018, https://itif.org/publications/2018/08/16/gdpr-freeloaders-why-other-countries-should-fight-back.
156. Certainly, a consent decree is no small punishment. It can confine a company to stagnant business practices, deter them from taking risks, and create greater barriers to new firms by subjecting them to costly, cumbersome, and complex de facto regulations under threat of potential lawsuits. Castro and McQuinn, "How and When Regulators Should Intervene."
157. Ibid.
158. "Gramm-Leach Bliley Act," (Federal Trade Commission (FTC), https://www.ftc.gov/enforcement/statutes/gramm-leach-bliley-act.
159. Ally Marotti, "Shutterfly Lawsuit Tags Illinois As Battleground in Facial Recognition Fight," *Chicago Tribune*, September 21, 2017, accessed December 18, 2018, https://www.chicagotribune.com/business/ct-biz-biometrics-shutterfly-lawsuit-20170920-story.html.

Acknowledgments

The authors wish to thank the following individuals for providing input to this report: Rob Atkinson, Randolph Court, and Alex Key. Any errors or omissions are the authors' own.

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 itif.org.