US Data Privacy Law: A Disparate Landscape in Need of Consolidation

Even before the EU General Data Protection Regulation (GDPR) brought attention to the issue of data privacy, the United States already had one of the most complex regulatory approaches to privacy, having implemented different laws and regulations by industry (e.g., healthcare, banking, education) and by state. The definitions, rules and controls required to protect data vary widely, depending on the industry sector. For instance, in the United States, financial data are governed by the Gramm-Leach-Bliley Act of 1999 (GLBA), and health information is governed by the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

In the wake of GDPR, and prior to the introduction of any federal-level legislation, individual US states began to pass legislation to protect the personal data of their residents, adding to the already complex regulatory requirements. At this point, 19 US states have active, pending or proposed legislation related to consumer privacy rights.[1] Some of these laws, such as the California Consumer Privacy Act of 2018 (CCPA), closely reflect the articles of GDPR, while others deviate significantly. Further complicating matters are another 26 states' privacy laws and breach notification and reporting laws, resulting in a regulatory landscape that is almost impossible for organizations to understand, let alone comply with and manage.[2]

The complexity of and contradictions between state laws and the volume of legal and regulatory requirements in the United States result in both an unnecessary expense to enterprises (and potentially to consumers, due to noncompliance and to enterprises passing this expense on to customers) and an obstacle to achieving common goals such as protecting end users' privacy, empowering users' rights over their data (including education and transparency regarding the use of data), and ensuring that privacy laws and policies keep up with changing technology. These disparate privacy laws only create more confusion, leading to misapplied standards and controls. The United States needs a common sense federal-level response that supersedes all state laws to bring clarity and simplification to the data privacy environment.

The following considers the various US federal-level proposals that will not only impact US organizations, but also international organizations that collect, process or store the personal

Jacob Nix, CISA, CCSFP, CPA, ISO 27001 LI
Is the chief executive officer of RISCPoint Advisory Group, a risk, compliance and technology advisory firm. He has published several articles in the *ISACA® Journal*.

Pascal A. Bizarro, CISA
Is an associate professor of accounting in the department of accounting and management information systems at Bowling Green State University (Ohio, USA). He has published several articles in the *CPA Journal*, the *ISACA Journal* and *Internal Auditing*.

Enjoying this article?

- Read *California Consumer Protection Act (CCPA) Audit Program. https://www.isaca.org/ccpa-audit-program*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

information of US citizens similarly to how GDPR affects organizations outside of the European Union. Although the focus of this discussion is the need to reform US privacy law, also provided is an analysis of the areas of greatest risk and the tools that enterprises can use to protect themselves now. It is a complex environment to navigate, but many resources have been developed to help enterprises build the right privacy posture through education, design and implementation.

Trends Driving the Increase in Data Privacy Laws

Recent trends in US data privacy legislation and regulation have been influenced by a number of actions and, in some cases, inaction. Some attribute the increase in state-specific US privacy laws to GDPR, claiming that US legislative activity is a reaction to the perception that the European Union is more advanced.[3] Others argue that it is a long-overdue recognition of the value of data and consumers' right to privacy.[4]

The mass collection of private data from consumers has been happening for years. Prior to 2016, very few data-collection efforts were transparent or targeted, and there was little justification for collecting the data. The reason behind this trend was simple: There was a common perception that enterprises could generate more revenue by collecting and selling consumers' data than they could by selling their services directly to customers.[5] Customer data can be obtained by asking customers for data, by indirectly tracking customers and by adding other sources of customer data to an enterprise's source, and some have said that a robust business strategy needs all three of these approaches.[6] This perspective has been a large contributor to enterprises' efforts to collect as much information as they can, regardless of the means or the transparency of the process.

Profiting from data is much more widespread than some might expect, reaching far outside the traditional tech community and even into the US government. One report found that some US state Departments of Motor Vehicles had been collecting drivers' personal information and selling it to insurance and towing organizations and even private investigators. The departments were legally permitted to do this under the terms of the US Driver's Privacy Protection Act of 1994 (DPPA).[7] Illustrating the value of such data, the Florida Department of Highway Safety and Motor Vehicles generated US$77 million in data sales revenue in 2017.[8]

"PROFITING FROM DATA IS MUCH MORE WIDESPREAD THAN SOME MIGHT EXPECT, REACHING FAR OUTSIDE THE TRADITIONAL TECH COMMUNITY AND EVEN INTO THE US GOVERNMENT."

Although the commercial model of using and selling data is a common one in the United States, it can cause problems when an enterprise must comply with GDPR or other laws, such as the CCPA. A key principle of data privacy regulations is that the individual retains ownership of personal data; data do not belong to the enterprise collecting or processing them. The timeline for compliance with data privacy laws should have started yesterday, according to one legal expert.[9] Enterprises should start by focusing their efforts on general principles, such as basic data mapping, and then move on to the specific laws that apply, as there are now numerous jurisdictions with tailored rules based on industry or organization. While US organizations are subject to fines, what often is a greater penalty for failing to comply with these regulations is the cost of private litigation, in addition to the potential loss of reputation. Rather than looking at legislation and trying to make it inapplicable, enterprises should assume that the law will apply, if it does not already, and take a cross-functional approach involving their general counsel and compliance functions.[10]

Why Is the United States' Disparate Privacy Landscape a Problem?

When GLBA and HIPAA were adopted in the 1990s, consumers' online activity was much different from today. Outside of these sensitive and highly

regulated areas, there was little to no incentive for enterprises to collect and monetize consumer data. However, the value of data has skyrocketed.

Not all data are created equal, but data privacy and the laws that govern it should be. In the past, it made sense to have specific regulatory guidance covering only the most sensitive data; however, a standardized approach similar to GDPR makes sense in today's environment. In the United States, a nationwide privacy law that identifies special categories of data and applies comprehensive restrictions and safeguards would bring clarity and simplicity, allowing enterprises to better respond and adhere to data privacy standards.

Ensuring data privacy and implementing technical and operational controls that meet evolving standards are difficult enough without having to analyze to which laws an enterprise must adhere. According to a 2018 survey of the International Association of Privacy Professional (IAPP) membership, complying with GDPR required enterprises to increase their internal privacy teams and to spend, on average, more than US$3 million to implement a GDPR program.[11] Among the enterprises surveyed, more than half stated that they were far from being fully GDPR compliant or never would be. These results are concerning, as the survey concluded that compliance with GDPR is a key driver in maintaining business-to-business relationships. Additionally, to reduce privacy risk, 75 percent of the respondents had created a data protection officer (DPO) position to lead organizational privacy practices.[12] Potential stringent legislation passed by the US Congress similar to GDPR and CCPA would cost the US economy more than US$122 billion per year, but a more targeted set of regulations addressing consumer protection would reduce that cost considerably. (See **figure 1** for a comparison of the costs of stringent vs. targeted regulations.)[13]

Given this complexity, how can the United States fix its data privacy law problem? On 12 March 2020, the Consumer Data Privacy and Security Act (CDPSA) became the latest proposed privacy bill in the United States, following the US Consumer Online Privacy Rights Act (COPRA) and the US Consumer Data Privacy Act (CDPA).[14] None of these bills, in their current state, are sufficient to serve as a comprehensive federal law. One of these proposals needs to be expanded and adopted to replace the data privacy and security aspects of the GLBA, HIPAA, DPPA and other industry-specific privacy laws.

One of the first challenges to overcome is determining which entities will be required to follow the standards. At first glance, the most recent bill (CDPSA) appears to be the strongest starting point, as it has wider applicability than the other two; it includes all entities subject to the jurisdiction of the US Federal Trade Commission (FTC), common carriers and nonprofit organizations.[15] However, the question becomes whether all entities should be treated equally. For example, should small organizations be held to the same requirements and penalties (for failure to comply) as large enterprises?

Figure 1—Potential Business Impact of Stringent vs. Targeted Regulations

Costs of Unnecessarily Stringent Regulations	US$ Billion/Year
Compliance costs	$6.4
Additional privacy personnel	$0.4
Privacy audits	$7.2
Right to access, deletion, data portability and recertification	$2.7
Duplicative enforcement	$1.9
Productivity loss due to pop-up notifications	
Market inefficiencies	
Reduced access to data	$71.0
Lower advertising effectiveness	$32.9
Total	**$122.5**
Costs of Targeted Regulations	**$6.5**

> THE MEASURES NEEDED TO PROTECT ENTERPRISES AND IMPLEMENT BEST PRACTICES ARE OFTEN EXPENSIVE, AND LEADERSHIP OFTEN CONSIDERS THEM A COST RATHER THAN AN INVESTMENT.

Another challenge is that although the key principles appear to be consistent, the bills vary in some of their specific details, such as definitions, enforcement and extent. For example, in terms of obtaining consent from an individual for data processing, when is consent required (i.e., when data are being processed for a specific purpose or when they are being transferred to third parties)? Can consent be implicit, or must it always be explicit? Are consent requirements different for personal vs. sensitive data (and how is each type defined)?

Despite these challenges, one key area of agreement is that enterprises must be aware of and transparent about the data they collect and create an environment that enforces strong privacy practices, including assigning ownership of and responsibility for these practices to a DPO.

How Can Enterprises Protect Themselves?

Privacy is similar to other historical regulatory and compliance challenges faced by enterprises and those in charge of complying with regulations. The measures needed to protect enterprises and implement best practices are often expensive, and leadership often considers them a cost rather than an investment. Given the fines for noncompliance that have been proposed, however, the fines alone are often not enough to make a meaningful case when presenting a cost-benefit analysis to leadership.

The support and buy-in of leadership are best obtained by explaining the intricate relationship among security, compliance and privacy. By illustrating this balance and providing an analysis that is holistic and showcases potential costs that are less tangible, such as future fines, reputational loss and downtime, privacy can be supported by one of the most compelling numbers that exists: the cost of a data breach.

Although privacy laws impose fines as a result of a data breach, they do not have any further correlation to the cost of a data breach, but it is simple to explain that the more data collected, and depending on the manner in which they are collected, the greater the risk exposure and, ultimately, the greater the impact of a data breach. This explanation can convince leadership of the need to invest in system improvements, compliance functions and design work. When outlining the potential costs of a breach, it is helpful to cite statistics. For instance, in 2019, the average cost of a data breach in the United States reached US$8.19 million; these costs can be divided into three types: direct, indirect and hidden (**figure 2**).[16]

Once a business justification has been established for addressing data privacy, the approach must be tailored to the specific environment. Enterprises can

Figure 2—Types of Data Breach Costs

Cost Type	Examples
Direct	Detection, notification of breach Share price decrease Legal services fees Forensic services fees Postbreach response Customer relations activities Financial reimbursement/settlement costs
Indirect	Damaged reputation Less interest in company stock Increase in third-party insurance
Hidden	Increased future technology investments Decreased interest from top talent

be classified as either data controllers or data processors. A data controller is "the natural or legal person, public authority, agency or other body that, alone or jointly with others, determines the purposes and means of processing personal data."[17] Data controllers are responsible for the fulfillment and execution of the vast majority of compliance requirements pertaining to data privacy. A data processor is "the natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller."[18] The data processor's responsibility is to assist the data controller in protecting the personal data in its possession and to ensure that a sufficient level of technical security control has been implemented to protect the confidentiality, availability and integrity of the personal data processed. Navigating these distinctions and the specific requirements of each can be difficult, so it is useful to develop an enterprise control framework that incorporates compliance, security and privacy considerations.

This approach gives enterprises, regardless of their size, a basis for evaluating, designing and operating an environment efficiently and effectively. It also lends itself well to what is considered the standard in data privacy: International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) ISO/IEC 27701:2019. This was the first international standard devised to certify the implementation and effectiveness of a privacy program. The framework has already received praise from large multinational organizations, including Microsoft.[19]

ISO/IEC 27701 provides a framework for managing privacy; however, the prerequisite for implementation and certification under ISO/IEC 27701 is the standard for an information security management system: ISO/IEC 27001. Similar to the building of enterprise control frameworks, ISO has built its privacy standard as an add-on to its information security standard.

As enterprises continue to try to mitigate their risk related to privacy, and regardless of the standard they use to measure themselves, a holistic approach to not only privacy but also to security and compliance is the key to minimizing risk and implementing the strongest defense in the event of a breach.

Adding Value Through Assessment: An Audit Perspective

Enterprises often struggle to determine the first step in designing a privacy program or even identifying where they are in that journey. This is where an internal audit or outsourced compliance evaluation, such as a privacy capabilities and maturity assessment, can add value. Risk, as defined by the US National Institute of Standards and Technology (NIST), is a measure of the extent to which an entity is threatened by a potential circumstance or event.[20] Risk is typically a function of the adverse impacts that would arise if the circumstance or event occurs and the likelihood of its occurrence. A risk assessment allows an enterprise to quantitatively apply a measure of risk based on the data being processed. For instance, if the enterprise processes large-scale quantities of special categories of data, it should implement enhanced security controls to protect those data.

"ENTERPRISES OFTEN STRUGGLE TO DETERMINE THE FIRST STEP IN DESIGNING A PRIVACY PROGRAM OR EVEN IDENTIFYING WHERE THEY ARE IN THAT JOURNEY."

To create a consistent and repeatable process for enterprises to implement and assess their capabilities and maturities relative to data privacy, NIST released its Privacy Framework.[21] The framework, which allows enterprises to measure the success of a privacy program, can be divided into three main parts:

1. **Core**—Defines privacy protection activities and is broken down into five categories: identify-P, govern-P, control-P, communicate-P and protect-P
2. **Profiles**—Defines the specific activities within each core category that an enterprise can choose to implement to achieve its business objectives

3. **Implementation tiers**—Defines the current implementation status of the selected profiles, ranging from Tier 1—Partial to Tier 4—Adaptable. The implementation tiers help enterprises optimize the resources allocated to manage privacy risk.

An inherent relationship exists between security and privacy, and it is impossible to ensure an appropriate level of data privacy without strong technical security controls to complement the privacy program. Naomi Lefkovitz, a senior privacy policy adviser at NIST, stated, "Merely adopting a good security posture does not necessarily mean that an organization is addressing all its Privacy needs."[22] Regulatory and compliance requirements are continuing to evolve, which means that enterprises must implement continuous improvement programs to ensure an appropriate level of security based on the data being processed. Just because an enterprise is meeting IT compliance requirements does not mean that it has eliminated all its vulnerabilities.[23]

> "A REVAMPED AND UNIFORM LAW AT THE FEDERAL LEVEL WITH ADDITIONAL APPENDICES TO ALLOW FOR INDUSTRY OR STATE-SPECIFIC REQUIREMENTS IS NEEDED."

Conclusion

The privacy landscape in the United States continues to fluctuate as state and federal laws are introduced, revised, removed and, at times, entered into a period of enforcement. This complex environment has made it difficult for organizations to maintain an adequate understanding of the various laws and regulations they are required to meet.

A revamped and uniform law at the federal level with additional appendices to allow for industry or state-specific requirements is needed. This would allow organizations dealing with personal information to focus on implementing safeguards, rather than spending time and resources developing the adequate understanding of what applies to their organization and how to meet it.

Although this shift to an organized approach for developing and implementing privacy laws at the federal level is an aspiration of many because it would reduce wasted effort within the business community, it is unlikely to be seen in the near future. Therefore, there should exist a best practice approach to addressing privacy within an organization's environment. This includes performing an assessment of the current state and then developing an enterprise-level approach to privacy, security and compliance to allow for a robust solution that is flexible, scalable and as efficient as possible in an inefficient landscape.

Endnotes

1 Noordyke, M.; "US State Comprehensive Privacy Law Comparison," International Association of Privacy Professionals (IAPP), *https://iapp.org/resources/article/state-comparison-table/*

2 National Conference of State Legislatures (NCSL) "Data Security Laws: Private Sector," *www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx*

3 Kimbol, A.; "Emerging Trends: What to Expect from Privacy Laws in 2020," *CPO Magazine*, 29 January 2020, *https://www.cpomagazine.com/data-protection/emerging-trends-what-to-expect-from-privacy-laws-in-2020/*

4 Menand, L.; "Why Do We Care So Much About Privacy?" *The New Yorker*, 18 June 2018, *https://www.newyorker.com/magazine/2018/06/18/why-do-we-care-so-much-about-privacy*

5 Eddy, M.; "How Companies Turn Your Data Into Money," *PC Magazine*, 10 October 2018, *https://www.pcmag.com/news/how-companies-turn-your-data-into-money*

6 Uzialko, A.; "How Businesses Are Collecting Data (and What They're Doing With It)," *Business News Daily*, 3 August 2018, *https://www.businessnewsdaily.com/10625-businesses-collecting-data.html*

7 Cox, J.; "DMVs Are Selling Your Data to Private Investigators," Vice, 6 September 2019, *https://www.vice.com/en_us/article/43kxzq/dmvs-selling-data-private-investigators-making-millions-of-dollars*

8 WFTS Staff, "Florida Is Selling Drivers' Personal Information to Private Companies and Marketing Firms," WXYZ Detroit, 11 July 2019, *https://www.wxyz.com/news/national/florida-is-selling-drivers-personal-information-to-private-companies-and-marketing-firms*

9 Ehret, T.; "Interview: Data-Privacy Compliance Timeline Is 'Yesterday,' Leading Tech Lawyer Says," *Reuters*, 8 October 2019, *https://www.reuters.com/article/bc-finreg-data-privacy-cynthia-cole-inte/interview-data-privacy-compliance-timeline-is-yesterday-leading-tech-lawyer-says-idUSKBN1WN1KG*

10 *Ibid.*

11 EY, *IAPP-EY Annual Privacy Governance Report 2018*, USA, 2018, *https://www.ey.com/Publication/vwLUAssets/ey-iapp-ey-annual-privacy-gov-report-2018/$File/ey-iapp-ey-annual-privacy-gov-report-2018.pdf*

12 *Ibid.*

13 McQuinn, A.; D. Castro; "The Costs of an Unnecessarily Stringent Federal Data Privacy Law," Information Technology and Innovation Foundation (ITIF), 5 August 2019, *https://itif.org/publications/2019/08/05/costs-unnecessarily-stringent-federal-data-Privacy-law*

14 Fennessy, C.; "US Sen. Moran's New Privacy Bill: Stacking Up the Federal Proposals," IAPP, 20 March 2020, *https://iapp.org/news/a/us-sen-morans-new-privacy-bill-stacking-up-the-proposals/*

15 *Ibid.*

16 Puranik, M.; "What Is the Cost of a Data Breach?" *Forbes*, 2 December 2019, *https://www.forbes.com/sites/forbestechcouncil/2019/12/02/what-is-the-cost-of-a-data-breach/#6a347dda29e7*

17 Intersoft Consulting, Article 4 GDPR Definitions, paragraph 7, EU General Data Protection Regulation, Belgium, 2018, *https://gdpr-info.eu/art-4-gdpr/*

18 Intersoft Consulting, Article 4 GDPR Definitions, paragraph 8, EU General Data Protection Regulation (GDPR), Belgium, 2018, *https://gdpr-info.eu/art-4-gdpr/*

19 Naden, C.; "Tackling Privacy Information Management Head On: First International Standard Just Published," International Organization for Standardization (ISO), 6 August 2019, Switzerland, *https://www.iso.org/news/ref2419.html*

20 National Institute of Standards and Technology (NIST), Computer Security Resource Center, USA, *https://csrc.nist.gov/glossary/term/risk*

21 National Institute of Standards and Technology (NIST), "NIST Releases Version 1.0 of Privacy Framework," USA, 16 January 2020, *https://www.nist.gov/news-events/news/2020/01/nist-releases-version-10-privacy-framework*

22 National Institute of Standards and Technology (NIST), "NIST Releases Version 1.0 of Privacy Framework," USA, 16 January 2020, *https://www.nist.gov/news-events/news/2020/01/nist-releases-version-10-privacy-framework*

23 Bartley, M.; "Why Prioritizing Cybersecurity Makes Compliance Easier," *Forbes*, 13 January 2020, *https://www.forbes.com/sites/forbestechcouncil/2020/01/13/why-prioritizing-cybersecurity-makes-compliance-easier/#643036f3162e*