Accounting for Enterprise Cloud Technologies in Comprehensive U.S. Privacy Legislation

Accounting for Enterprise Cloud Technologies in Comprehensive U.S. Privacy Legislation

Executive Summary

The United States has the opportunity to advance a modern legal framework that protects individuals and enhances understanding and trust in technology, yet is flexible enough to keep pace with the wide range of new technology-based services that rely upon data. As a central component of this framework, Congress should enact comprehensive privacy legislation based on the Organisation for Economic Co-operation and Development (OECD) Fair Information Practices and backed by strong enforcement powers for the Federal Trade Commission (FTC). Importantly, strong privacy legislation should recognize that technology is not monolithic; that enterprise cloud service providers, in particular, handle consumer data in a materially different way than parties that directly control consumer data; and that data processors, such as enterprise cloud service providers, should be regulated differently than data controllers. Such a law would harmonize privacy protection within the U.S. by creating a consistent approach that consumers could depend on, no matter in which state they live, thereby avoiding the prospect of litigation over what law applies. It would be interoperable with other global privacy regimes, such as the European Union's (EU) General Data Protection Regulation (GDPR). And it would facilitate consumer trust in digital services and the free flow of data, both of which are vital for unlocking the potential of groundbreaking innovations. By protecting consumers with a reliable and robust privacy framework flexible enough to capture differences among rapidly evolving technologies such as enterprise cloud services, Congress can set the stage for the next wave of technological innovation in data-powered services.

Introduction

At Workday, we believe privacy is a fundamental right. Privacy has been vital to Workday from our very beginning. As a provider of financial management and human capital management applications, we assist our enterprise customers in empowering employees with the information and tools they need to enhance their skills and become more strategic in their roles. Our planning and analytics applications help our customers make more informed decisions by leveraging intelligent technologies to get the insights they need into their business.[1] As with many enterprise cloud providers, our customers subscribe to our services but remain in control of their data and how it is used. Strong privacy protections are not only important to our business, they also go hand in hand with the adoption of intelligent technologies. After all, people will let their data be used for machine learning only if they have confidence that their data will be protected and handled consistent with their expectations. Strong privacy controls are vital to establishing trust in new technology.

When developing new products, Workday embeds privacy protection measures throughout the development process: we have made privacy by default[2] part of our standard requirements for new features and products.[3] Workday third-party audit reports and standards certifications provide tangible evidence about how we protect data. As a part of our strong, ongoing commitment to privacy and protecting our customers' data, Workday not only has provided features to enable our customers to comply with the GDPR,[4] but we also were among the first companies to certify to the EU-U.S. Privacy Shield, as well as the first U.S. company to achieve the APEC Privacy Recognition for Processors.[5] Our Binding Corporate Rules for Processors has also received EU approval.[6]

Policymakers around the world are grappling with how best to provide individuals with control over their personal information as technological tools become more powerful. Congress has been deeply engaged in a legislative process that includes multiple hearings on this issue.[7] Similarly, California is considering amendments to its newest privacy bill,[8] and GDPR has been in effect for nearly a year. Given the pace of technological innovation and the abundance of services available to both individuals and enterprises, creating a cohesive and sufficiently flexible privacy framework may seem like a daunting task. However, the U.S. can build on its lengthy privacy law tradition to advance a model privacy framework that protects the individual's fundamental right to privacy, enhances consumer understanding and trust in technology, and facilitates the free flow of data essential to providing individuals and businesses with the best possible services. As a leading provider of enterprise cloud applications for finance and human resources that delivers analytics applications designed for the world's largest companies, educational institutions, and government agencies, Workday offers this paper to assist policymakers in developing a robust U.S. approach to privacy that accounts for cloud-enterprise service providers and is interoperable with GDPR and other frameworks around the world—while flexible enough both to keep pace with the wide range of businesses harnessing data to provide new services and to enable technology innovation that will empower those businesses.

Part I of this paper explains the urgent need for comprehensive privacy legislation in the U.S. in light of the potential of data-driven technologies and the long-standing history of protecting privacy rights in the U.S. Part II describes the core structure of the cloud ecosystem, using Workday services as an example, to explain the distinct considerations presented by enterprise cloud services. Part III outlines the Workday proposal for a comprehensive privacy framework in the U.S. that would be workable for cloud service providers and explains why legislation based on the OECD Fair Information Practices, interoperable with GDPR, and backed by strong enforcement measures is essential to unlocking the potential of groundbreaking new technologies while also prioritizing the consumer trust essential to the success of these technologies.

It's Time for the U.S. to Enact Comprehensive Privacy Legislation to Ensure Protection of Individuals and Their Personal Information, Regardless of Where They Live or with Whom They Interact

Innovative technologies, such as machine learning, are poised to deliver sweeping changes across nearly all sectors of the economy, transforming the way enterprises conduct business, governments deliver services, and individuals live their daily lives. Machine learning relies on the pooling of multiple, diverse, and thoughtfully selected data sources, that together can determine important patterns and generate valuable insights. Put simply, data is its lifeblood. But the availability of quality, useful data in turn depends largely on one critical factor: consumers' ability to trust that their privacy will be properly protected.

Globally, the privacy landscape is shifting toward stronger regulation of data. In May 2018, the EU implemented GDPR, updating the way EU countries approach consumer privacy regulation. Beyond the EU, countries across the globe are developing their own omnibus, comprehensive privacy laws. For instance, in August 2018, Brazil implemented a data privacy regulation modeled on GDPR,[9] joining Argentina, Uruguay, Mexico, Chile, Colombia, Costa Rica, Nicaragua, and Peru as the most recent Latin American country to implement a comprehensive data protection law.[10] In summer 2018, India released a draft of its own GDPR-based privacy legislation[11] and may soon join Australia, Hong Kong, Japan, Macao, Malaysia, New Zealand, the Philippines, Singapore, South Korea, and Taiwan as the most recent Asia-Pacific country to enact a comprehensive data protection law.[12]

This trend toward formalizing stronger privacy protections exists within the U.S. as well. Most notably, last year, California passed the California Consumer Privacy Act ("CCPA"), the most sweeping state-level privacy law to date.[13] On the heels of the CCPA, other states are also introducing data privacy and cybersecurity laws.[14] In recent legislative sessions, some states, such as Washington, considered privacy legislation that was similar to GDPR.[15]

In this context, the U.S. has a valuable opportunity to update its approach to protecting consumer privacy and enact its own comprehensive privacy legislation at the federal level. Not only would such a step bring the U.S. in line with efforts worldwide, it would also continue the deep tradition in the U.S. of protecting individual privacy rights. Indeed, the concern for individual privacy rights has long been a feature of U.S. law. At the founding of the nation, the Fourth Amendment enshrined the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizure" from the government. At the end of the nineteenth century, Louis Brandeis published a seminal law review article that extended the concept of privacy to relations among private parties.[16] And in the 1970s, the Department of Health, Education, and Welfare published the Fair Information Practices Principles, which would ultimately serve as the foundation for the Organisation for Economic Co-Operation and Development's ("OECD") Fair Information Practices (FIPs), adopted in 1980.[17]

Despite this long-standing recognition of individual privacy rights in the U.S., the lack of a modern, comprehensive federal consumer privacy law has created a "patchwork" system of privacy laws in the U.S. These laws consist primarily of Section 5 of the Federal Trade Commission ("FTC") Act, state laws, and federal-level sector-specific laws. The FTC uses Section 5 of the FTC Act—and state attorneys general use state analogs to the FTC Act that exist in all 50 states[18]—to prohibit "unfair or deceptive acts or practices"[19] in the area of consumer privacy.

Under its Section 5 authority, the FTC has brought enforcement actions, including 75 general privacy lawsuits, addressing a wide range of privacy issues, such as spam, social networking, behavioral advertising, pretexting, spyware, peer-to-peer file sharing, and mobile.[20]

In addition to Section 5 of the FTC Act, a handful of sector-specific federal laws govern privacy and data security issues related to particular types of personal data. These include the Children's Online Privacy Protection Act of 1998 (COPPA), which regulates the online collection of children's personal information;[21] the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which regulates the protection of individually identifiable health information held by certain entities;[22] the Gramm-Leach-Bliley Act of 1999 (GLBA), which imposes privacy and data security obligations on financial institutions;[23] the Fair Credit Reporting Act (FCRA), which regulates the collection, dissemination, and use of "consumer report" information;[24] the Family Educational Rights and Privacy Act (FERPA), which regulates student records;[25] the Telemarketing and Consumer Fraud and Abuse Prevention Act, which regulates telemarketing;[26] and the Video Privacy Protection Act of 1998 (VPPA), which creates liability for knowing disclosure of information about a particular person requesting or obtaining particular video materials.[27]

While these laws together create a privacy protection framework that is stronger than it is often given credit for, the patchwork approach presents distinct disadvantages. Most notably, individuals' rights in the U.S. may depend on factors as varied as who they are, the state where they live, the entity with which they are interacting, and the type of personal data being processed. As a result, it is challenging for individuals to understand their rights and remedies and how their information is used, protected, and shared. Furthermore, the amalgam of sector-specific laws makes it difficult for other countries to assess the protections available for data transferred to the U.S., and feeds concerns that U.S. law is out of step with the global shift toward stronger data protection.

Congress should therefore seize this moment to reexamine the privacy framework in the U.S. and enact a new federal privacy law that enshrines key privacy protections, standardizes expectations for individuals and entities, and facilitates the free flow of information essential to providing the possible services across the internet ecosystem, in particular, by cloud enterprise service providers.

Comprehensive Privacy Legislation Should Be Compatible with the Enterprise Cloud Ecosystem

Meaningful individual control over personal information must be the goal of federal privacy legislation in order to match changes in technology and to be interoperable with frameworks around the world. Thus far, much of the discussion around federal privacy legislation has rightly focused on dynamics between an enterprise and an individual end user. It is important to bear in mind, however, that while critically important, these dynamics alone represent only part of the picture. A full picture includes an understanding of the enterprise cloud ecosystem and the business-to-business transactions at its core.

Cloud Technology Is Transforming the U.S. Economy

Across industries, U.S. businesses are increasingly using cloud technologies to lower costs, boost productivity, and foster innovation. Over 90 percent of U.S. firms use some form of cloud technology, and two-thirds of these firms use cloud components for a significant portion of their overall IT architecture.[28] In the past two decades, the cloud economy has nearly tripled in size.[29] U.S. companies are leaders in the provision of cloud services to meet this demand, which is expected to increase in 2019 to a $206.2 billion worldwide market for public cloud services.

Enterprise cloud solutions in particular have provided significant benefits, and as a result, companies are increasingly switching to them. Currently, 77 percent of enterprises have at least one application or a portion of their enterprise computing infrastructure in the cloud, and 15 percent of enterprises intend to adopt cloud applications and platforms in the next 12 months.[30]

The majority of these enterprises are looking to cloud technologies both to reduce costs and to enable their digital business models.[31] Analysts predict that by 2020, approximately two-thirds of all software, services, and technology spending will be cloud-based.[32]

More broadly, the cloud market's growth has contributed billions of dollars to the U.S. economy, with cloud technology estimated to have added $214 billion to U.S. GDP in 2017 alone.[33] Cloud technology supported 2.15 million jobs that same year.[34] The benefits of cloud services are not limited to one region, industry, or type of business. Rather, adoption of cloud technologies has occurred across the country and in every broad industry group and provided unique advantages to small businesses because of the cloud's affordability and flexibility.[35] By lowering operational costs and allowing an entity to scale up or down as needed, cloud technologies empower small businesses to compete with large firms in both domestic and foreign markets.[36]

Lastly, cloud services drive innovation. Cloud services enable businesses to use advanced technologies without the burden of owning the infrastructure that supports the tools. By avoiding these high up-front costs, a business can instead quickly explore and deploy emerging technologies and new ideas. For instance, over 80 percent of companies surveyed in a 2018 CompTIA report stated that cloud technologies enhanced their automation initiatives.[37] The benefits of cloud technologies included providing access to new tools, lowering the cost of exploring new technology, and enabling the internal team to focus on innovation.[38] In driving new opportunities for companies to use their IT operations, cloud services continue to directly and indirectly facilitate the U.S.'s role as a global technology leader.

Enterprise Cloud Services Have a Distinct Architecture

Despite its importance, the fundamental nature of cloud computing is often poorly understood. In general, cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (for example, networks, servers,

storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.[39] Various models of cloud computing services exist, but particularly important within the cloud ecosystem are enterprise cloud technologies.

Enterprise cloud technologies provide a computing environment for businesses that offers enhanced performance, reduced cost, and superior security. They are typically run using a SaaS model. Under SaaS models, customers receive the capability to use the cloud provider's applications, which run on cloud infrastructure, and they can access the applications using a thin client interface, such as a web browser. Importantly, the customer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, or storage. Certain cloud services do, however, offer customers access to user-specific application configuration settings.[40]

Workday itself offers cloud-based tools for financial management, human capital management, planning, and analytics. When using these tools, customers remain in full control of the data entered into Workday services. They also remain in control of all setup and configurations, such as what approvals are needed for expense reports or who has to sign off on pay changes. Because customers control their own data, they can perform tasks such as monitoring all business transactions and examining historical data and configuration changes.[41]

Workday services follow a "one-to-many" model, meaning all customers receive the exact same version of the Workday service. The one-to-many model revolves around the principle of the Power of One, which encapsulates the notion that a single cloud architecture enables one experience, one security model, and one community—and thereby delivers a superior customer and end-user experience.

This approach offers three key advantages for customers: simplicity, scalability, and security. End users can seamlessly use applications across multiple devices.[42] In addition, customers can bring data in at scale from any source and analyze it without having to leave Workday.[43] Under this approach, all customer data is treated as sensitive data and all data is encrypted at rest.[44] Moreover, this approach provides Workday customers with a transparent view into how their data is protected: rather than having to review fragmented security solutions with potentially inconsistent controls, the single security model in Workday for its core services allows for easy auditing and certification for its customers.[45]

Other enterprise cloud service providers, such as Okta, Twilio, and Zendesk, also provide tools for enterprise customers to streamline operations and ensure secure user experiences. These providers may offer identity management solutions for businesses, such as single sign-on and multifactor authentication,[46] or provide communications or customer support platforms that enable companies to quickly and easily connect with their customers.[47] As enterprise cloud service providers, they also take steps to limit their access to end-user data. Okta only populates the fields necessitated by an application when provisioning a user account for a service and discloses to that user what information has been made available to any offerings.[48] Zendesk explicitly states that it does not use customer content for any purpose other than providing, maintaining, and improving its services (or as otherwise required by law).[49] Similarly, Twilio does not sell end users' personal information or share it with third parties unless instructed or permitted to do so by a business.[50] In addition, these enterprise cloud service providers safeguard data with industry-standard encryption and keep their information security practices up-to-date with third-party audits and compliance with certification programs offered by the Cloud Security Alliance, the Privacy Shield Framework, and the International Organization for Standardization.[51]

Distinguishing Features of Enterprise Cloud Services

Enterprise cloud services have several distinctive features. First, the customers of enterprise cloud providers are enterprises—not individuals. Consequently, enterprise cloud providers typically do not interface with individuals, and many enterprise cloud services, such as Workday, are contractually prohibited from viewing their customers' data, except with the customer's permission in instances necessary for the provision of technical support services at the customer's request.

The business models of enterprise companies differ from others in the digital economy in some important respects. For example, Workday and many other enterprise cloud providers do not monetize user data by selling advertising. Instead they sell subscriptions to a service. Customers remain in control of their data and how it is used. Moreover, because customer trust is vital, cloud enterprise companies like Workday often compete on privacy, seeking to provide strong privacy and data security protections to ensure customers feel comfortable entrusting their sensitive business information with them. As a result, privacy controls are not an add-on feature; they are embedded in the service and business model.

Thus, fundamentally, cloud enterprise providers act in most instances as what GDPR would classify as "processors," while their customers act as "controllers." A controller is the entity that determines the purposes, conditions, and means of the processing of personal data, while the processor is an entity that processes personal data on behalf of the controller. This distinction is of paramount importance, as it recognizes the critical limitations of cloud service providers' interactions with end users and their data. Blurring the distinction between controllers and processors risks creating consumer confusion by failing to identify for end users exactly which entity is ultimately responsible for deciding what data is collected, how it is used, and why it is shared. As a result, consumers might not know to which entity they should turn to exercise control over their own data.

These features have significant policy implications. In particular, they underscore that rapidly evolving technologies are not monolithic. Different services interact with data in different ways. Successful privacy regulation must at least account for these differences and at best reflect them in a meaningful and nuanced way. Such a regime will allow for continued success in providing critical services, as well as the opportunity for continued innovation in the future.

A Comprehensive Privacy Framework in the U.S. Must Be Robust, Interoperable, and Consistent with the U.S. Legal Tradition

Workday proposes that Congress pass federal privacy legislation in the U.S. that is based on the OECD Fair Information Practices, interoperable with GDPR, and backed by strong enforcement measures in a manner that captures the distinct and critically significant features of the enterprise cloud system and cloud technologies more broadly.

Federal Privacy Legislation Should Include Strong Individual Rights Based on the OECD Fair Information Principles

The well-established OECD Fair Information Practices (FIPs)[52] should be the basis for a U.S. privacy framework, as they include core data privacy rights that are consistent with the current approach to privacy in the U.S., while remaining flexible enough to support country-to-country variation and strong enough to provide international harmonization.[53] A federal privacy law based on the OECD principles will also ensure fair treatment of individuals and their personal information, regardless of where they live or with whom they interact.[54]

The FIPs cover all of the core tenants of data privacy rights: data collection, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability.

They consist of eight principles:[55]

- **Collection Limitation:** There should be limits to the collection of personal data, and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
- **Data Quality:** Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete, and kept up-to-date.
- **Purpose Specification:** The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
- **Use Limitation:** Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified in accordance with the purpose specification principle, except with the consent of the data subject or by the authority of law.
- **Security Safeguards:** Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure of data.
- **Openness:** There should be a general policy of openness about developments, practices, and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data and the main purposes of their use, as well as the identity and usual residence of the data controller.
- **Individual Participation:** Individuals should have the right: (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to them; (b) to have communicated to them data relating to them (i) within a reasonable time; (ii) at a charge, if any, that is not excessive; (iii) in a reasonable manner; and (iv) in a form that is readily intelligible to them; (c) to be given reasons if a request made under part (a) and (b) is denied and to be able to challenge such denial; and (d) to challenge data relating to them and, if the challenge is successful, to have the data deleted, rectified, completed, or amended.
- **Accountability:** A data controller should be accountable for complying with measures which give effect to the principles stated above.[56]

The FIPs provide a widely shared common baseline for the 35 countries that are OECD members.[57] While the FIPs directly influenced the EU's Data Protection Directive in 1995, these principles are effectively restated in the recent GDPR, which took effect on May 25, 2018.[58] Article 5 of GDPR, which lists the "Principles relating to processing of personal data," includes all of the FIPs principles, except Individual Participation, which is referenced elsewhere in GDPR.[59] Additional GDPR articles elaborate on these principles and explain the responsibilities of data controllers, many of which reflect the OECD Guidelines. For example, the accountability standards in both the FIPs and GDPR place a greater emphasis on the responsibility of controllers to demonstrate that personal data is processed appropriately.[60] To date, many other countries have modeled their data protection laws off of the OECD FIPs, including Australia, New Zealand, Canada, and Japan.[61] The Asia-Pacific Economic Corporation ("APEC") privacy framework is also largely inspired by the OECD FIPs.[62]

Furthermore, the FIPs are sufficiently flexible to support country-to-country variation. Taking the form of eight concise principles, the FIPs provide countries with the ability to interpret the principles and apply them in a way that best aligns with their country's internal systems and goals. For example, the Collection Limitation principle states that any personal data collected should be obtained by lawful and fair means but leaves flexibility by not specifying what "lawful" or "fair" must entail.[63]

Whereas Article 6 of GDPR contains six circumstances under which processing is considered lawful, including when the data subject has given consent and when processing is necessary for the performance of a contract,[64] different definitions of lawful processing may be appropriate in different jurisdictions. Although the FIPs provide the foundation for a comprehensive privacy framework, they are not so prescriptive that they hinder country-specific tailoring to meet local needs.

The FIPs are also sufficiently strong to provide international harmonization to ensure that personal data can flow freely across borders in a cloud-enabled world. The principles cover important concepts such as consent and access rights, providing data subjects rights similar to those already present in frameworks like GDPR. They also establish limitations that are meant to minimize the likelihood of data being mishandled or inappropriately disclosed, such as the Collection Limitation and Use Limitation principles and the Security Safeguards principle. The enactment of a federal law adopting the OECD FIPs would likely place U.S. law on a pathway to being deemed "adequate" in the EU and thus promote the continued transfer of data between continents.

Moreover, a law based on the OECD FIPs will ensure fair treatment of individuals and their personal information, regardless of where they live or with whom they interact. Consumers should not only be able to expect fairness and transparency across the entities that process their data within their country[65] but also from entities across countries. While existing privacy protections in the U.S. are meaningful, the privacy protections an individual receives should not depend on where that individual is located. Thus, a U.S. law based on the OECD FIPs will strike the right balance between the need to facilitate data flows that spur innovation and investment and the imperative to protect consumers from harm.

Federal Privacy Legislation Should Be Interoperable with GDPR

In addition to being based on the OECD FIPs, U.S. privacy legislation should seek to be interoperable with GDPR, which is designed to harmonize data privacy laws across Europe and strengthen consumer privacy rights.[66] Given their shared roots, GDPR's key requirements align squarely with the OECD FIPs. GDPR encompasses all eight of the OECD principles, most of which are expressly stated in the regulation's list of principles relating to the processing of personal data.[67] Like the OECD FIPs, the final principle in GDPR's list is accountability, which requires the controller to "be responsible for, and be able to demonstrate compliance with," the rest of the principles.[68] The OECD principle of Individual Participation is addressed separately, in the section of GDPR covering the rights of data subjects.[69] These rights include the right to access personal data, the right to rectification, and the right to erasure,[70] which overlap considerably with the individual rights provided by the FIPs.[71]

In addition to providing individuals with greater protections around their data, GDPR requires organizations to change how they store, handle, and share data. As a result, several thousands of companies have already restructured their privacy programs to comply with GDPR. Enacting a federal privacy law in the U.S. that is interoperable with the EU is necessary because it advances the dual objectives of promoting the free flow of data and recognizing the critical distinction between controllers and processors.

Advancing the Free Flow of Data

At a minimum, GDPR-interoperable federal legislation will help ensure that the U.S. can continue to benefit from the enormous opportunities afforded by the free flow of data between the EU and the U.S. Optimizing the potential of new technologies and their attendant economics benefits depends on a healthy and robust flow of data across national boundaries.

A substantial body of evidence establishes that digital trade increases GDP and creates jobs. Cross-border data flows added an estimated $2.8 trillion to world GDP in 2014, surpassing the impact of global trade in goods.[72] In the EU alone, the value of the market for data-related products and services was estimated at almost €60 billion (2% of GDP) in 2016 and could grow to €106 billion (4% of GDP) by 2020.[73] A large number of firms participate in this market, including over 250,000 data companies (for example, organizations whose main activity is the production and delivery of data-related products or services)—a figure that could grow to 360,000 by 2020. EU data companies employed 6.1 million data workers in 2016; by 2020, that number could reach 10.4 million.[74]

More concretely, without free data flows, enterprise cloud services such as Workday's cannot reach their full potential. For instance, Workday applications give customers real-time insights into their organizations, allowing them to make decisions based on data rather than guesswork. Being in the cloud also means that customers have secure access to their financial and workforce data whenever and wherever they need it, on any device. For employers, this translates to an ability to better manage the business, and for employees, it simplifies many daily transactions and democratizes access to critical data. These features require analysis and computation across a customer's employee base, which is often global in reach.[75]

U.S. privacy legislation should be designed to facilitate the free flow of data, given its broad-sweeping significance. Legislation that is interoperable with GDPR helps achieve this objective. In particular, notwithstanding the EU's recognition of the importance of digital trade,[76] GDPR still places restrictions on transfers of personal data to third countries.[77] However, no additional safeguards, restrictions, or formalities apply to transfers of personal data to countries or organizations that are recognized by the EU as having an "adequate" level of privacy protection. One of the primary ways in which an organization can be found to meet this adequacy requirement is by certifying to the U.S.-EU Privacy Shield Framework.

The EU-U.S. Privacy Shield Framework was designed by the U.S. Department of Commerce and the European Commission to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the EU in support of transatlantic commerce. On July 12, 2016, the European Commission deemed the EU-U.S. Privacy Shield Framework adequate to enable data transfers under EU law.[78] The Privacy Shield program, administered by the Commerce Department, enables U.S.-based organizations to join the Privacy Shield Framework by self-certifying to the Department of Commerce and publicly committing to comply with the Framework's requirements—a commitment that is enforceable under U.S. law.

Because the Privacy Shield principles align closely with the heightened requirements of GDPR, legislation that is interoperable with GDPR may facilitate on a broad scale the ability of U.S.-based organizations to certify to the Privacy Shield Framework—and thus, promote the free flow of data between the U.S. and the EU. The existing disparate structure of U.S. privacy law makes it difficult for other countries to determine whether gaps exist in protection. Moreover, the Privacy Shield Framework provides for an annual review process to assess the Privacy Shield's functioning, implementation, supervision, and enforcement; this review process is currently under way. Given the uncertainty the annual review process may introduce, parties on both sides of the Atlantic would benefit from a more permanent solution to cross-border data flows and privacy protections. Ultimately, the right legislation in the U.S. may pave the way for a national-level adequacy determination, once other related issues, such as national security concerns, have been addressed as well.

Recognizing the Controller Versus Processor Distinction

Differentiating between controllers and processors is essential because the distinction establishes a clear allocation of roles and responsibilities and helps clarify complex situations where data is processed by more than one entity, as is commonly the case with cloud services.

GDPR offers one way to clearly distinguish between these two roles and imposes specific obligations on each.[79] In particular, GDPR defines "controller" as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data…"[80] It then defines "processor" as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller."[81] The U.S. could look to this model for its own legislation.

Regardless of whether the U.S. adopts privacy legislation that is closely aligned with GDPR, it should differentiate between these two types of entities and the roles they play. The primary obligation for ensuring compliance with the privacy law should rest with the controller. The controller is the entity that holds the direct relationship with the end user; determines what information to collect and for what purposes; and decides how it is used, with whom it is shared, and under what terms. By contrast, the processor merely acts on behalf of the controller and does not make the key decisions affecting compliance with core data protection obligations. Accordingly, a processor's main obligation should be to follow the instructions of the controller and ensure the security of the personal data it processes.

Clearly differentiating between controllers and processors is also necessary to avoid confusion that may arise from the complex system of relationships that underlie modern data processing operations. Maintaining this allocation would also avoid disturbing the existing economic and contractual relationships between processors and controllers. Making controllers primarily responsible for ensuring compliance with privacy law also comports with common sense, because both regulatory authorities and individuals will know to whom to turn to in case of a problem. Finally, given that the new Brazilian privacy law,[82] the pending Indian law,[83] and the proposed Washington state law[84] all differentiate between controllers and processors, recognizing this distinction will help ensure U.S. federal privacy law remains in line with global developments.

Promoting Interoperability Without Replicating Shortcomings

Given the strong history of privacy law in the U.S., the U.S. is well positioned to chart its own path with federal privacy legislation. Indeed, a robust U.S. privacy framework could also serve as a model for other countries that are also considering changes to their data protection frameworks. In any event, the correct legislative solution for the United States cannot include copying and pasting GDPR into the U.S. Code, because GDPR still leaves room for improvement on measures both procedural and substantive. U.S. legislation should avoid replicating these shortcomings, even as it presents an overall interoperable framework. Moreover, because so many aspects of GDPR deal with unique and idiosyncratic characteristics of the EU, adopting it into U.S. law would be a poor fit. The U.S. should instead establish an independent legislative model that seeks workable consistency with existing models where possible.

As a threshold matter, although GDPR was designed to harmonize privacy regulation across the EU, it still permits meaningful discretion by member countries that can result in inconsistent standards. In particular, of GDPR's 65 substantive articles, 30 explicitly permit member states to diverge from the standard set forth in the article.[85] For example, Article 8 of GDPR mandates a particular consent regime for treating personal data acquired online from children under the age of 16. At the same time, it states that each member state "may provide by law for a lower age for those purposes provided that such lower age is not below 13 years."[86] The potential for variation in this article has been realized: Austria has selected under 14 as the threshold, while the United Kingdom has selected under 13. As a result, entities that wish to collect personal data from children in Europe will need to familiarize themselves with the age threshold in each member state and adapt their procedures accordingly. Moreover, the level of protection a child receives for her data depends on the specific EU member state in which she is located. Thus, GDPR still permits in meaningful ways the differentiation among member state laws that harmonization was supposed to eliminate.

Given that the option for divergence exists in 30 of the substantive articles, approximately 46 percent of GDPR's substantive articles expressly permit member states to engage in such variation.[87]

Relatedly, GDPR fails to provide for a single enforcement authority. Under Article 51, each member state must establish a public authority responsible for monitoring the application of GDPR, defined as a "supervisory authority."[88] Furthermore, under Article 83, the authority to impose fines lies with each member nation's supervisory authority.[89] As a result, the enforcement of GDPR may vary, based on each supervisory authority's interpretation of the regulation. Not only does this variation create uncertainty for entities operating across the EU but it also creates uncertainty for the individuals who use the services of such entities. If a company is found to have violated privacy laws, the degree to which the company is held responsible for the violation of an individual's privacy rights may depend on where enforcement against that company is pursued.

More substantively, some of GDPR's requirements are ill suited for the realities of the cloud ecosystem. For instance, GDPR requires that processors obtain consent from controllers prior to engaging subprocessors.[90] This obligation makes little sense for one-to-many enterprise cloud models such as Workday's. Because one-to-many models entail the provision of the same service to all customers, the subprocessor used will be the same for all customers. Nevertheless, GDPR still requires the cloud enterprise provider to obtain consent for each subprocessor from each of the thousands of customers it might have. An equally effective and far more efficient measure to ensure subprocessors adhere to privacy requirements is simply to require that a processor contractually obligate its subprocessors to comply with its own requirements and to remain responsible for the subprocessor's compliance. GDPR already includes these requirements,[91] rendering the subprocessor consent requirement unnecessarily cumbersome and, ultimately, superfluous.

In addition, GDPR includes detailed audit provisions for processors and subprocessors.[92] While specific provisions may, in theory, assist entities in ascertaining compliance, to the extent entities are responsible for their processors' privacy practices, audit rights should be subject to commercial negotiation rather than prescribed by statute. Finally, GDPR includes a "right to erasure," also known as a "right to be forgotten."[93] While the provision's intent to increase an end user's control over her data is well meaning, the "right to erasure" may risk sweeping facts and ideas of public concern out of the social sphere. As a result, it is arguably inconsistent with the uniquely strong U.S. respect for free speech and First Amendment rights.

The European framework also does not map perfectly onto U.S. legal culture or law—given, for example, the tension between GDPR's "right to be forgotten" and the First Amendment. But identical approaches are not necessary for effective coexistence. It is preferable for the U.S. to adopt its own strong approach toward protecting consumer privacy that is fundamentally consistent with the GDPR approach in order to maximize the benefits of the global nature of internet-based connectivity for individuals and enterprises alike. Consistency is necessary to help make consumers' expectations and understanding of their rights clear across the board, to minimize risks of consumer confusion, and to ensure that the level of privacy protection an individual receives is not contingent on where she is physically located.

Federal Privacy Legislation Should Be Strongly Enforced by the FTC

Concern for the privacy rights of individuals has long been a feature of U.S. law and legal commentary, and the U.S. has a rich and often underappreciated privacy law history. Moving forward, legislation in the U.S. should maintain the best of these traditions by bolstering the FTC's ability to serve as the primary privacy regulator.

Within the limits of its existing statutory authority under Section 5 of the FTC Act, the FTC has done an admirable job protecting consumer privacy in the U.S. In addition to pursuing 75 general privacy enforcement actions,[94] the FTC has also developed policy recommendations related to consumer privacy and data security and authored over 60 reports, based on independent research as well as workshop submissions and discussions.[95] The Commission has also conducted studies, hosted public workshops, developed educational materials for consumers and businesses, testified before the U.S. Congress, commented on legislative and regulatory proposals that affect consumer privacy, and worked with international partners on global privacy and accountability issues.[96]

Notwithstanding these valuable efforts, there are meaningful shortcomings in the FTC's ability to provide muscular enforcement of privacy rights. First, under its existing statutory authority, the FTC may not issue a fine on a first offense; rather, it may issue a fine only when a company violates a consent order.[97] Specifically, under Section 5(b) of the FTC Act, the Commission may, in the first instance, challenge "unfair or deceptive act[s] or practice[s]" (or violations of other consumer protection statutes) through maintenance of an administrative adjudication. When there is "reason to believe" that a law violation has occurred, the Commission may issue a complaint setting forth its charges. If the respondent elects to settle the charges, it may sign a consent agreement (without admitting liability), consent to entry of a final order, and waive all rights to judicial review. Only if a respondent violates the final Commission order is it liable for a civil penalty for each violation, as set forth in Commission Rule 1.98(c).[98]

Second, the FTC has only limited rulemaking authority, and no rulemaking authority specific to general privacy regulation though some statutes grant it specific authority such as COPPA,[99] the Do-Not-Call Implementation Act of 2003,[100] the Fair and Accurate Credit Transactions Act of 2003,[101] and the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003.[102]

Because the Commission lacks rulemaking authority with respect to general privacy matters, however, its privacy guidance is delivered piecemeal primarily through its enforcement actions. This nonuniform approach takes a long time to develop and creates gaps where the FTC has chosen not to enforce or where new issues arise.

Furthermore, the FTC's enforcement actions are based on its authority to police "unfair and deceptive" conduct. In practice, the FTC's reliance on its broad authority has left room for companies to challenge its application in privacy and data security regulation. For instance, in the recent FTC v. Wyndham Worldwide Corp. case, Wyndham challenged the FTC's authority to bring data security cases under Section 5. While the Third Circuit held that, based on the procedural posture and facts of the case, Wyndham did have fair notice of its potential liability under the statute, the court's statutory fair notice analysis illustrated a tension between effective FTC regulation of data security practices and constitutional notice requirements.[103] Future courts facing more-difficult factual circumstances will likely have to grapple with this tension in a way the Third Circuit was able to avoid.[104] More importantly, this uncertainty harms not just enterprises but consumers as well—leaving them with an incomplete picture of what will ultimately constitute a violation of their data privacy or security rights.

Congress should strengthen the FTC's privacy regulatory authority with new legislation. In particular, it should authorize the FTC to promulgate privacy-specific regulations. To be sure, granting the FTC expanded rulemaking authority does not mean Congress should abdicate its duties; Congress should still develop robust privacy legislation based on the OECD FIPs that provide baseline protections. At the same time, however, Congress should also empower the FTC to expand on and clarify those basic rights through rulemaking. The FTC can use this authority to help make sure the law stays current with ever-evolving technologies and practices while, at the same time, keeping regulation grounded to the baseline protections enumerated in federal legislation.

Congress should also empower the FTC with civil penalty authority, permitting the agency to impose penalties in response to a first offense. Civil penalty authority would strengthen the FTC's regulatory authority by creating a stronger deterrent to violating the privacy laws. As long as Congress passes clear legislation and the FTC enacts clear rules based on that legislation, civil penalties offer a more potent solution for vindicating privacy rights.

Conclusion

Ultimately, comprehensive privacy legislation must revolve around reinforcing consumers' trust in the entities with which they share their data online. As a next step, Workday offers this paper in the hopes of advancing the dialogue currently underway among policymakers, regulators, industry, and consumers about how best to unlock the tremendous benefits that evolving technology offers while prioritizing the privacy of individuals to bolster that trust.

Endnotes

1 *See* "Four Technology Trends That Will Inform the 2019 Policy Agenda" (February 25, 2019) https://blogs.workday.com/four-technology-trends-that-will-inform-the-2019-policy-agenda/technology-trends-that-will-inform-the-2019-policy-agenda

2 *See*, e.g., Article 25.2 of Regulation (EU) 2016/679 of the European Parliament and 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), 2016 O.J. L 119/1 [hereinafter "GDPR"], *available at* https://eur-lex.europa.eu/eli/reg/2016/679/oj ("The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each spe cific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.")

3 *See* "GDPR: Privacy by Design at Workday," Workday (August 30, 2017), https://blogs.workday.com/gdpr-privacy-design-workday/.

4 *See* "Countdown to GDPR," Workday (May 25, 2017), https://blogs.workday.com/countdown-to-gdpr/. When it comes to GDPR compliance, Workday and our customers both have responsibilities: our customers as data controllers and Workday as a data processor. A controller is the entity that determines the purposes, conditions, and means of the processing of personal data, while the processor is an entity which processes personal data on behalf of the controller. In addition to Workday's own compliance obligations under GDPR as a processor of customers' personal data, Workday also assists customers in meeting their obligations as data controllers under GDPR in a variety of ways.

5 *See* "Workday Certifies to Privacy Shield," Workday (August 1, 2016), https://blogs.workday.com/workday-self-certified-on-day-one-of-privacy-shield/; Privacy Shield List, Department of Commerce (last visited March 22, 2019), https://www.privacyshield.gov/participant_search. *See also* "Workday Is First Company to Attain New Asia- Pacific Privacy Certification," Workday (December 10, 2018), https://blogs.workday.com/workday-is-first-company-to-attain-new-asia-pacific-privacy-certification/.

6 *See* "Workday Receives EU Approval on Binding Corporate Rules," Workday (May 2, 2018), https://blogs.workday.com/workday-receives-eu-approval-on-binding-corporate-rules/; "List of Companies for Which the EU BCR Cooperation Procedure Is Closed," European Commission (May 24, 2018), *available at* https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=613841.

7 *See, e.g.*, "Oversight of the Federal Trade Commission: Strengthening Protections for Americans' Privacy and Data Security: Hearing before the Subcommittee on Consumer Protection and Commerce of the House Committee on Energy and Commerce," 116th Congress (2019); "Privacy Principles for a Federal Data Privacy Framework in the United States," Hearing before the Senate Commerce Committee, 116th Congress (2019).

8 *See, e.g.*, A.B. 1355, 2019–20 Regular Session (California 2019); S.B. 753, 2019–20 Regular Session (California 2019); A.B. 25, 2019–20 Regular Session (California 2019); A.B. 873, 2019–20 Regular Session (California 2019).

9 Lei Ordinária No. 13.709, de 14.08.18 ("Lei Geral de Proteção de Dados Pessoais"), *available at* https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

10 Lisa J. Sotto, *Privacy and Cybersecurity Deskbook* § 1.03[A] (2019).

11 The Personal Data Protection Bill, 2018, Ministry of Electronics and Information Technology (Draft released on July 27, 2018), *available at* https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill%2C2018_0.pdf.

12 *See* Sotto, *supra* note 10, at § 1.03[B].

13 California Consumer Privacy Act, A.B. 375 (California 2018) (amended by S.B. 1121 (California 2018)).

14 Hawaii, Massachusetts, Maryland, New Mexico, and Rhode Island recently introduced bills that largely mirror the CCPA but utilize different enforcement mechanisms. *See* S.B. 418, 30th Legislature, 2019 Session. (Hawaii 2019); S.D. 341, 191st General Court (Massachusetts 2019); S.B. 613, 2019 Legislature, 439th Session (Maryland 2019); S.B. 176, 54th Legislature, 1st Session (New Mexico 2019); and S. 0234, 2019 General. Assembly, January Session (Rhode Island 2019).

15 Joseph O'Sullivan, "Washington Senate Approves Consumer-Privacy Bill to Place Restrictions on Facial Recognition," *The Seattle Times* (March 6, 2019), https://www.seattletimes.com/seattle-news/politics/senate-passes-bill-to-create-a-european-style-consumer-data-privacy-law-in-washington/; María Miranda, "Bill Introduced to Protect, Regulate Personal Data in Puerto Rico," Caribbean Business (March 25, 2019), https://caribbeanbusiness.com/bill-introduced-to-protect-regulate-personal-data-in-puerto-rico/.

16 *See* Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," 4, *Harvard Law Review*, Rev. 193 (1890).

17 *See* "Records, Computers and the Rights of Citizens," report of the Secretary's Advisory Committee on Automated Personal Data Systems, U.S. Department of Health, Education, and Welfare (July 1, 1973), *available at* https://aspe.hhs.gov/report/records-computers-and-rights-citizens [hereinafter "HEW Report"].

18 *See, e.g.*, Iowa Code §§ 714.16 through 714.16A; Kentucky Rev. Stat. Ann. §§ 367.110 through 367.990 (West); New Jersey Stat. Ann. §§ 56:8-1 through 56:8-91 (West); South Dakota Codified Laws §§ 37-24-1 through 37-24-35.

19 15 U.S.C. § 45.

20 *See* "Privacy & Data Security Update: 2018," Federal Trade Commission, 3 (March 15, 2019), https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2018/2018-privacy-data-security-report-508.pdf [hereinafter "2018 FTC Privacy & Data Security Update"].

21 15 U.S.C. §§ 6501–6506.

22 Pub. L. No. 104-191, 110 Stat. 1936 (1996).

23 15 U.S.C. §§ 6801–6809 (2012).

24 *See* 15 U.S.C. § 1681 *et seq*.

25 20 U.S.C. § 1232.

26 15 U.S.C. § 6101–6108.

27 18 U.S.C. § 2710(a)(3).

28 "Cloud Computing and IT Operations," CompTIA, 1 (May 2018), https://www.comptia.org/resources/cloud-computing-trends-research ("Nearly half of all companies claim that 31% to 60% of their IT systems are cloud-based… 91% of companies claim to be using some form of cloud computing").

29 "Examining the Economic Contributions of the Cloud to the United States Economy," Internet Association, 6 (March 5, 2019), https://internetassociation.org/publications/examining-economic-contributions-cloud-united-states-economy/.

30 *See* "State of Enterprise Cloud Computing, 2018," *Forbes* (August 30, 2018), https://www.forbes.com/sites/louiscolumbus/2018/08/30/state-of-enterprise-cloud-computing-2018/#5448c327265e/.

31 *See Ibid.*

32 "Roundup of Cloud Computing Forecasts, 2017," *Forbes* (April 29, 2017), https://www.forbes.com/sites/louiscolumbus/2017/04/29/roundup-of-cloud-computing-forecasts-2017/#38732a8e31e8 ("By 2018, at least half of IT spending will be Cloud-based, reaching 60% of all IT infrastructure, and 60–70% of all Software, Services, and Technology Spending by 2020.").

33 "Examining the Economic Contributions of the Cloud to the United States Economy," *supra* note 29.

34 *See Ibid.*

35 Nicholas Bloom and Nicola Pierri, "Research: Cloud Computing Is Helping Smaller, Newer Firms Compete," *Harvard Business Review* (August 31, 2018), https://hbr.org/2018/08/research-cloud-computing-is-helping-smaller-newer-firms-compete.

36 "Ahead of the Curve: Lessons on Technology and Growth from Small-Business Leaders," The Boston Consulting Group, 10–11 (October 2013), http://image-src.bcg.com/Images/Ahead_of_the_Curve_Oct_2013_tcm9-94245.pdf ("Cloud-based capabilities enable [SMEs] to go head-to-head with companies of any size by providing a host of powerful, pay-as-you-go capabilities. Enterprisewide solutions such as infrastructure, platform, and software as a service (IaaS, PaaS, and SaaS) allow SMEs to build synthetic scale incrementally and flexibly. They eliminate the need for big, upfront capital expenditures in favor of more manageable, ongoing operational expenses. This applies not only to IT purchases but also to the cost of entering a market. A company with these resources at its disposal no longer needs to open a new office or a new factory in a foreign country in order to gain access to its capabilities and customers.").

37 "2018 Trends in Cloud Computing," CompTIA, 8 (May 2018), https://www.comptia.org/resources/cloud-computing-trends-research.

38 *See Ibid.*

39 "The NIST Definition of Cloud Computing," National Institute of Standards and Technology (NIST), 2 (September 2011), https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf.

40 *See Ibid.*

41 *See* "Architectural Security," Security and Trust, Workday (last visited March 24, 2019), https://www.workday.com/en-us/company/security-and-trust.html.

42 *See The Workday Tech Strategy*, Workday, Chapter 1 (last visited March 24, 2019), https://www.workday.com/en-us/pages/ebook-it-workday-tech-strategy.html.

43 *See Ibid.*

44 *See The Value of One Security Model*, Workday (last visited March 25, 2019), https://www.workday.com/en-ca/pages/video-one-security-model.html.

45 *See Ibid.*

46 *See* "Products in the Okta Identity Cloud" in "Protect the Identities of Your Workforce and Customers," Okta (last visited March 23, 2019), https://www.okta.com/products/.

47 *See* "Services" in "Twilio Products," Twilio (last visited March 23, 2019), https://www.twilio.com/products; "Product" in "The Zendesk Suite," Zendesk (last visited March 23, 2019), https://www.zendesk.com/suite/.

48 *See* "Privacy by Design" in "The GDPR, Identity, and Your Organization," Okta (September 26, 2017), https://www.okta.com/blog/09/2017/preparing-for-GDPR/.

49 *See* "How Does Zendesk Use Service Data?" in "EU Data Protection" (last visited March 24, 2019), https://www.zendesk.com/company/customers-partners/eu-data-protection/.

50 *See* "When and Why We Share Your Personal Information or Your End Users' Personal Information," in "Twilio Privacy Statement," Twilio (last visited March 25, 2019), https://www.twilio.com/legal/privacy#when-and-why-we-share-your-personal-information.

51 *See Security and Reliability*, Okta (last visited March 23, 2019), https://www.okta.com/security/; *Twilio Trust & Security*, Twilio (last visited March 23, 2019), https://www.twilio.com/security; *Zendesk Security*, Zendesk (last visited March 23, 2019), https://www.zendesk.com/product/zendesk-security/.

52 The OECD Fair Information Principles ("FIPS") emerged in the 1980s as an outgrowth of privacy developments in the U.S.. In 1973, the U.S. Department of Health, Education, and Welfare (HEW) published the Fair Information Practices Principles in response to rising "concern about the harmful consequences that may result from uncontrolled application of computer and telecommunications technology to the collection, storage, and use of data about individual citizens." HEW Report, *supra* note 17, at Preface.

In 1980, the Organisation for Economic Co-operation and Development ("OECD") used these core HEW fair information principles and built upon them to create a set of eight Fair Information Principles. The FIPs were set forth in the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and agreed upon by member countries, including the U.S., through a consensus and formal ratification process. *See* "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," OECD (last visited March 24, 2019), http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm, [hereinafter "OECD Guidelines"]. Ultimately, the FIPs became the basis of the EU's Data Protection Directive, adopted in 1995. *See* Jason Albert, "U.S. Privacy Law: A Short History," LinkedIn (June 22, 2018), https://www.linkedin.com/pulse/us-privacy-law-short-history-jason-albert/; *see also* OECD Guidelines, *supra*.

53 *See* "Workday Supports Comprehensive Privacy Legislation in the US and Globally," Workday (June 25, 2018), https://blogs.workd ay.com/workday-supports-comprehensive-privacy-legislation-in-the-us-and-globally/; *see also* "Draft Framework for Data Protection in the United States from Consumer and Privacy Organizations" (October 9, 2018), https://epic.org/testimony/congress/CPOs_to_SCC_US_Data_Protection_Framework_Oct2018.pdf ("Baseline federal legislation should be based on familiar Fair Information Practices, such as the widely followed OECD Privacy Guidelines."); "Public Interest Privacy Legislation Principles" (November 12, 2018), https://newamericadotorg.s3.amazonaws.com/documents/Public_Interest_Privacy_Principles.pdf ("Legislation should… require all entities that collect, store, use, generate, share, or sell… data both online and offline to comply with Fair Information Practices…").

54 *See Ibid.*

55 In 2013, the OECD updated the Privacy Guidelines for the first time since their launch in 1980. "OECD Privacy Guidelines," OECD (last visited March 24, 2019), http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm.

56 OECD Guidelines, *supra* note 52.

57 "Where: Global Reach," OECD (last visited July 31, 2019), http://www.oecd.org/about/membersandpartners/.

58 *See* GDPR Article 5; *see also* Robert Gellman, "Fair Information Practices: A Basic History," 11–12 (April 10, 2017), https://bobgellman.com/rg-docs/rg-FIPshistory.pdf.

59 *See* Gellman, *supra* note 58, 11–12.

60 *See* Monika Kuschewsky, "What Does the Revision of the OECD Privacy Guidelines Mean for Businesses?" (October 22, 2013), https://www.cov.com/~/media/files/corporate/publications/2013/10/what_does_the_revision_of_the_oecd_privacy_guidelines_mean_for_businesses.pdf.

61 *See Thirty Years After: The OECD Privacy Guidelines*, OECD (2011), http://www.oecd.org/sti/ieconomy/49710223.pdf.

62 *See APEC Privacy Framework*, APEC (2015), https://www.apec.org/-/media/APEC/Publications/2017/8/APEC-Privacy-Framework-(2015)/217_ECSG_2015-APEC-Privacy-Framework.pdf.

63 *See* OECD Guidelines, *supra* note 52.

64 *See* GDPR Article 6(1).

65 *See* Public Interest Privacy Legislation Principles, *supra* note 53.

66 *See Ibid.*

67 *See* GDPR Article 5 (including the following principles: "lawfulness, fairness and transparency," "purpose limitation," "data minimisation," "accuracy," "storage limitation," "integrity and confidentiality," and "accountability").

68 *See* GDPR Article 5(2).

69 *See* GDPR Articles 15–17; *see also* Gellman, *supra* note 58, 11–12.

70 *See* GDPR Articles 15–17.

71 These rights include an individual's right to have communicated to him data relating to him; to challenge such data; and if the challenge is successful, to have the data erased, rectified, completed, or amended. *See* OECD Guidelines, *supra* note 52.

72 *See* James Manyika *et al.*, "Digital Globalization: The New Era of Global Flows," McKinsey Global Institute, 4 (March 2016), *available at* https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows.

73 *See* European Parliament, Directorate-General for Internal Policies, *Data Flows–Future Scenarios: In-Depth Analysis for the ITRE Committee* (November 2017), *available at* http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/607362/IPOL_IDA(2017)607362_EN.pdf, 11.

74 *See Ibid.*

75 *See* "Why Workday Advocates the Free Flow of Data Throughout the EU," Workday (June 12, 2017), https://blogs.workday.com/why-workday-advocates-the-free-flow-of-data-throughout-the-eu/.

76 *See, e.g.*, "Towards a Digital Trade Strategy," report of the Commission on International Trade, 2017/2065 (INI) (November 29, 2017), *available at* http://www.europarl.europa.eu/doceo/document/A-8-2017-0384_EN.html?redirect.

77 *See* GDPR Articles 44–50.

78 *European Commission Implementing Decision (EU) 2016/1250 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*, 2016 O.J. (L 207), 1, *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.207.01.0001.01.ENG&toc=OJ%3AL%3A2016%3A207%3AFULL.

79 *See* GDPR Article 4(7) ("'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data…"); GDPR Article 4(8) ("'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller."). *See also* GDPR Article 24 ("Responsibility of the controller") and GDPR Article 28 ("Processor").

80 *See* GDPR Article 4(7).

81 *See* GDPR Article 4(8).

82 Lei Ordinária No. 13.709, de 14.08.18 ("Lei Geral de Proteção de Dados Pessoais"), *available at* https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm (English translation *available at* https://www.pnm.adv.br/wp-content/uploads/2018/08/Brazilian-General-Data-Protection-Law.pdf).

83 *The Personal Data Protection Bill, 2018*, Ministry of Electronics and Information Technology (draft released on July 27, 2018), *available at* https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill%2C2018_0.pdf.

84 S.B. 5376, 66th Legislature, 2019 Session (Washington 2019), *available at* http://lawfilesext.leg.wa.gov/biennium/2019-20/Pdf/Bill%20Reports/Senate/5376-S2%20SBR%20APS%2019.pdf.

85 *See* David Bender, "GDPR Harmonization: Reality or Myth?" International Association of Privacy Professionals (June 7, 2018), *available at* https://iapp.org/news/a/gdpr-harmonization-reality-or-myth/.

86 *See* GDPR Article 8(1).

87 *See* Bender, *supra* note 85.

88 *See* GDPR Article 51(1); GDPR Article 83(1).

89 *See* GDPR Article 83(1).

90 *See* GDPR Article 28(2) ("The processor shall not engage another processor without prior specific or general written authorization of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.").

91 *See* GDPR Article 28(4) ("Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.")

92 *See, e.g.*, GDPR Article 30.

93 *See* GDPR Article 17 ("The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay…").

94 *See* 2018 FTC Privacy & Data Security Update, *supra* note 19, 3.

95 *See Ibid.*

96 *See Ibid.*

97 *See* FTC Act, Section 5(l), 15 U.S.C. § 45(l) ("Any person, partnership, or corporation who violates an order of the Commission after it has become final, and while such order is in effect, shall forfeit and pay to the United States a civil penalty of not more than $10,000 for each violation, which shall accrue to the United States and may be recovered in a civil action brought by the Attorney General of the United States.").

98 *See* "A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority," Federal Trade Commission (last visited March 24, 2019), https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority.

99 15 U.S.C. §§ 6501–6506.

100 15 U.S.C. § 6101.

101 15 U.S.C. §§ 1681 *et seq.*

102 15 U.S.C §§ 7701–7713.

103 *See* 799 F.3d 236 (3d Circuit 2015); *see also* case comment "Third Circuit Finds FTC Has Authority to Regulate Data Security and Company Had Fair Notice of Potential Liability: FTC v. Wyndham Worldwide Corp.," 129, *Harvard Law Review* 1120, 1120 (2016).

104 *See* 129, *Harvard Law Review* 1120.

workday.

+1-925-951-9000 | +1-877-WORKDAY (+1-877-967-5329) | Fax: +1-925-951-9001 | workday.com