Hearing on

"Policy Principles for a Federal Data Privacy Framework in the United States"

Senate Committee on Commerce, Science, and Transportation

February 27, 2019, at 10:00 a.m.
Hart Senate Office Building
Room 216
Washington, DC

Testimony of Victoria Espinel
President and CEO
BSA | The Software Alliance

Testimony of Victoria Espinel

President and CEO, BSA | The Software Alliance

Hearing on "Policy Principles for a Federal Data Privacy Framework in the United States"

Good morning Chairman Wicker, Ranking Member Cantwell, and members of the Committee. My name is Victoria Espinel. I am President and CEO of BSA | The Software Alliance.

BSA is the leading advocate for the global software industry in the United States and around the world.[1] Our members are at the forefront of developing cutting-edge, data-driven services that have a significant impact on U.S. job creation and the global economy. I commend the Committee for holding this hearing on the important topic of a federal data privacy framework, and I thank you for the opportunity to testify on behalf of BSA.

This is the year to pass strong, consumer-centric privacy legislation, and BSA looks forward to working with this Committee to make it a reality. Privacy and security are core to establishing customer trust, which is necessary to realize the potential of the data economy to create jobs and improve lives.

We represent the enterprise perspective, meaning as you consider legislation, we urge you to remember that not all tech companies have the same business model. BSA companies don't rely on making money off of selling ads. They make money by selling products. They license software and sell services. They're partners with businesses of all sizes across every industry in the economy.

All of us care about privacy, and we particularly care about sensitive information. People may not mind if a photo of their dog is seen by the public. But people definitely care about outsiders tracking where they go, who they talk to, and which apps are sharing sensitive information with third parties without their knowledge. They care about their personal emails. They care about details of the business they've worked hard to build. They care about their private health and financial information. All of this information must be strongly protected.

That's why people choose our companies to protect their data. They entrust it to our companies, and BSA companies work very hard to keep that trust. That promise to protect your privacy is paramount. When you use Outlook to write an email, Microsoft is not reading your emails to serve you targeted ads. When you use Salesforce to manage your relationships with customers, your customer lists stay secret.

BSA companies want Congress to pass a clear and comprehensive national law that gives consumers the right to know, the right to control, and the right to choose what happens to their personal information; imposes obligations on companies to safeguard consumers' data and prevent misuse; and provides strong, consistent enforcement. Federal privacy legislation that includes these elements will protect consumer privacy interests, promote innovation, and promote global data flows.

Strengthening consumer privacy protections is a goal that BSA shares, and we urge you to pass strong data privacy legislation as soon as possible.

[1] BSA's members include: Adobe, Akamai, Apple, Autodesk, Bentley Systems, Box, Cadence, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, Siemens PLM Software, Slack, Splunk, Symantec, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

I. The Importance of Personal Data in the Digital Economy and the Widespread Benefits of Data-Driven Innovation

Over the last 20 years, consumers, businesses, and governments around the world have moved online to conduct business and access and share information. Services, including cloud computing, artificial intelligence (AI), and the Internet of Things, have transformed commerce, helping companies enter new markets and compete on a global scale. They have also delivered unprecedented efficiencies and considerable cost savings to every industry sector. As global leaders in the development of these data-driven products and services, BSA members prioritize the protection of consumers' personal data, and they understand that robust data protection is a key part of building consumer trust and promoting full participation in the digital economy.

The economic impact of software- and data-enabled innovation is enormous. In the United States, software contributes $1.14 trillion to GDP and supports 10.5 million jobs, with an impact in each of the 50 states and across a range of industries. Software-enabled technologies increasingly rely on data and, in some cases, personal data, to perform their intended functions. Nearly ubiquitous network connectivity, growth in the number of connected devices, and improvements in algorithms and analytical techniques have led to dramatic, data-driven improvements in our ability to solve difficult societal challenges, bringing significant and widespread benefits and go far beyond business models that rely primarily on the monetization of consumers' personal data.

For example, AI technologies are providing myriad benefits to small and large organizations across a wide swath of industries, as well as consumers and society as a whole. To make AI work in practice, developers need access to data to build, evaluate, and maintain their systems. AI is helping organizations solve complex, rapidly changing, global problems, including:

- **Cybersecurity.** AI tools are revolutionizing how companies monitor network security by improving cyber threat detection, analyzing malicious behavior patterns, and detecting malware in real time. AI is also helping analysts parse through hundreds of thousands of security-related events per day to weed out false positives and identify threats that warrant further attention by network administrators. By automating responses to routine incidents and enabling security professionals to focus on truly significant threats, AI-enabled cyber tools help enterprises stay ahead of their malicious adversaries.

- **Fraud Detection.** AI is improving fraud detection by recognizing suspicious behavior and providing companies with real-time information that helps to identify and investigate different types of fraud, reducing the losses caused by malicious actors by billions of dollars. These tools also protect consumers from the risk of fraudulent charges and from the frustration associated with "false declines."

- **Healthcare.** Software is helping medical networks coordinate care among hospitals, doctors, and health care facilities to reduce redundant care costs and improve health care quality. Additionally, AI is helping doctors predict patient risk for illnesses such as heart disease and create treatments.

- **Diversity and Inclusion.** AI is being used to promote inclusion. For instance, AI systems are at the heart of new devices and applications that can improve the lives of people with disabilities. AI is also helping people with vision-related impairments interpret and understand visual content, such as photos and their physical surroundings, opening new possibilities to navigate the world with increased independence and greater ability to engage in communities.

BSA companies use data in many other ways that help protect privacy and security. For example, services that help consumers and enterprises manage online identities to authenticate users not only provide strong security and protect privacy but also improve the user experience, making shortcuts that create vulnerabilities less attractive. Other BSA members provide privacy-enhancing technologies that

use, for example, data masking, enabling companies to reduce the sensitivity of data they hold and mitigate privacy and security threats.

Cloud computing services provided by BSA members also improve security by implementing state-of-the-art, multilayered defenses and allowing customers to compartmentalize datasets, thereby preventing a breach in one location from impacting the full dataset. BSA members know that the responsible deployment of these services requires dealing transparently with their customers. Users of these services entrust some of their most sensitive data – including personal data – with our members. As a result, privacy and security protections are fundamental parts of BSA members' operations.

Finally, BSA members provide services that help other organizations grow and thrive. From human resources management to design and engineering, our members use data to develop and improve their products for customers all over the world. Indeed, BSA members also help their customers compete in a complex, global environment. Many BSA members provide services that power other businesses, including start-ups and small- and medium-sized enterprises. These services are designed to enable compliance across this broad range of customers, allowing them to enter markets that might otherwise be prohibitively expensive. Global interoperability in privacy laws, in turn, supports these efforts.

Maintaining global data flows is critically important to realizing many of these benefits, as well as developing and using cloud computing services to their maximum advantage. Global data flows enable companies of all sizes to reach customers and find suppliers across the world. Cross-border data flows also help fuel data analytics, which can deliver limitless socially and economically beneficial results in myriad contexts, ranging from digital commerce to natural disaster response. For example, hospitals and other healthcare organizations often need to transfer personal data across borders for use in clinical support software, which analyzes electronic health records, health insurance claims, and data sets to help caregivers improve the effectiveness of medical treatments and reduce overall health risks.

In short, BSA members provide data-driven services that are driving U.S. and global economic growth, provide substantial societal benefits, and enable the protection of the privacy and security of consumers' personal data.

II. The Role of Federal Legislation

In addition to the experience that BSA members have with protecting personal data and complying with the EU General Data Protection Regulation (GDPR) and other privacy laws across the globe, BSA has a long history of engaging with industry, government, and other stakeholders to advance privacy protections.[2] For example, BSA has been an active participant in ongoing policy and framework development processes led by the Federal Trade Commission (FTC) and the Department of Commerce. BSA has also encouraged the U.S. government to discourage data localization measures and continue its efforts to facilitate cross-border data flows through frameworks such as the EU-U.S. Privacy Shield and the Asia-Pacific Economic Cooperation's Cross-Border Privacy Rules system. These efforts have been critical to developing the digital economy as well as privacy best practices.

Now, as consumers face increased difficulty in navigating a more complex technological landscape, and as data practices among companies vary widely, BSA supports federal privacy legislation to ensure that consumers receive appropriate privacy protections, organizations face clear obligations, and the United States maintains a strong position to protect global data flows.

More specifically, federal privacy legislation should achieve three goals: give consumers the right to know, the right to control, and the right to choose what happens to their personal information; impose

[2] *See generally* BSA | The Software Alliance, Privacy Framework (released Sept. 12, 2018), https://www.bsa.org/~/media/Files/Policy/BSA_2018_PrivacyFramework.pdf ("BSA Privacy Framework").

strong obligations on companies to safeguard consumers' data and prevent misuse; and provide strong, consistent enforcement.

A. Providing Strong Privacy Rights for Consumers: The Right to Know, the Right to Control, and the Right to Choose

Transparency. Federal legislation should require organizations to provide users of their services with clear and accessible explanations of their practices for handling personal data. Providing consumers with information that enables them to understand how an organization processes personal data directly supports the aim of giving them more control over their personal data.

However, providing this information in a manner that is helpful to consumers can be challenging.[3] Determining how best to provide information to consumers may depend, among other things, on the types of data at issue as well as the kind of services that an organization offers to consumers. Companies therefore need sufficient flexibility to communicate information about their data practices in order to best inform consumers. Still, there are certain types of information that in most, if not all, circumstances are useful to provide to consumers and therefore are worth considering incorporating into federal legislation as generally applicable requirements, including: (i) the categories of personal data that organizations collect; (ii) the type of third parties with whom they share data; and (iii) the description of processes the organization maintains to review, request changes to, request a copy of, or delete personal data.

Informed Choice. Consumers should be able to exercise appropriate control over their personal data. Although notice and choice alone may not address all privacy challenges, in appropriate settings, consumer choice still has an important role to play.

Organizations should provide consumers with sufficient information to make informed choices and, where practical and appropriate, the ability to opt out of the processing of personal data.

Organizations should consider the sensitivity of personal data at issue. Certain data, such as information about an individual's financial accounts or health condition, may be particularly sensitive. Requiring organizations to obtain affirmative express consent from consumers when collecting this sensitive information is appropriate under many circumstances.

Sensitivity-based obligations help to ensure that privacy protections comport with consumers' expectations, generally offering the strongest protections in settings that present the greatest risk of concrete harm to consumers. Personal data types that should be classified as sensitive are: precise geolocation data; unique, government-issued identifiers; biometric data; genetic data; financial account information; medical information; the contents of communications (with respect to an entity that is not an intended recipient of the communication); and personal data that relates to a consumer's racial or ethnic origin or sexual orientation.

Access, Correction, and Deletion. In light of the increasing challenges that consumers face in understanding the implications of choices and the growing range of circumstances in which implementing choice is infeasible, consumers should have other ways to improve their control over personal data. In particular, consumers should be able to request information about whether organizations have personal data relating to them as well as the nature of such data. In addition, consumers should be able to request a copy of the data, challenge the accuracy of that data, and, where relevant and appropriate, have the data corrected or deleted. With appropriate access to the personal data that organizations hold about them, consumers can make more informed decisions about whether and to what extent to use that

[3] *See, e.g.,* Notice and Request for Comments, Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 48,600, 48,601 (Sept. 26, 2018) (noting that "lengthy notices describing a company's privacy program at a consumer's initial point of interaction with a product or service" are part of the current "paradigm" of privacy notices).

organization's services. Organizations that determine the means and purposes of processing personal data should be primarily responsible for responding to these requests under federal privacy legislation.

Federal legislation should also set certain limits on the ability of consumers to request a copy of, access, correct, or delete personal data. In particular, companies must have the flexibility to deny these requests when the burden or expense of fulfilling a request would be unreasonable or disproportionate to the risks to the consumer's privacy. In addition, organizations should have the ability to deny access, correction, or deletion requests in order to promote other important interests, including compliance with legal requirements; the protection of network security and confidential commercial information; conducting research; and avoiding the infringement of privacy, free speech, or other rights of other consumers.

B. Establishing Strong Obligations for Companies to Safeguard Consumer Data and Prevent Misuse

Although it is important for federal legislation to give consumers better ways to make informed choices about personal data and exercise control over it, other measures may be necessary to ensure sufficient privacy protection. Organizations that handle personal data should have processes in place to ensure that their safeguards appropriately address privacy risks, including but not limited to the prevention of inappropriate uses of data, security breaches, and other incidents that may harm consumers' privacy. BSA therefore supports including security and accountability in federal privacy legislation.

Security. Data security is integral to protecting personal data and privacy. Currently, however, companies must navigate a complex tangle of data security laws, rules, and standards – some of which are difficult to decipher and apply, while others are in conflict with one another. To address these issues, federal privacy legislation should also establish a harmonized baseline data security standard.

A federal data security standard should require organizations to employ reasonable and appropriate security measures designed to prevent unauthorized access, destruction, use, modification, and disclosure of personal data based on the volume and sensitivity of the data, the size and complexity of the business, and the cost of available tools. A data security standard also should take into account the wide range of security risks that companies face, the rapidly changing nature of security threats, and the complexity of developing security standards. Accordingly, data security requirements must be flexible, and they should be consistent with internationally recognized standards that also are risk-based, technology-neutral, and outcome-focused.

Accountability. Accountability within organizations that handle personal information is also critical to effective data protection. The central objective in accountability is for organizations that process personal data to remain responsible for its protection, no matter where or by whom the data is processed. Policies and practices that govern how an organization as a whole handles personal data are essential to ensuring that the organization identifies relevant privacy risks and appropriately manages them. They also are essential to identify means that allow consumers effectively to exercise control over personal data. Specific elements that should underlie accountability include (i) designating persons to coordinate the implementation of these safeguards, including providing employee training and management; (ii) regularly monitoring and assessing such implementation; and (iii) where necessary, adjusting practices to address issues as they arise. Organizations should also employ governance systems that seek to ensure that personal data is used and shared in a manner that is compatible with stated purposes.

Each organization will have different lines of business and an array of other considerations that relate to how to structure and combine accountability practices. Therefore, providing flexibility in how organizations ensure their own accountability is important. More specifically, the use of any specific accountability mechanism should not be mandatory. Instead, privacy legislation should focus on the objectives of responsible data processing.

Notably, companies, including BSA members, are also using data in ways that both broaden inclusion, such as providing increased access to opportunities for people with learning disabilities or visual impairments, and helping other business customers understand better how the data and advanced

technologies they are using lead to a range of outcomes, enabling other companies to be more transparent about the services they provide. In service of these objectives, companies maintain safeguards to mitigate the risk of bias or unlawful discrimination.

Controller/Processor Distinction. As Congress establishes strong obligations for organizations to implement, providing clarity about an organization's role and responsibilities in the complex, dynamic, data-driven economy can complement enforcement efforts by promoting business arrangements that reinforce those responsibilities. The distinction between controllers, which determine the purposes for which personal data is processed, and processors, which perform storage, processing, and other data operations on behalf of controllers, is key to allowing organizations that handle personal data to clearly define their responsibilities.

It is appropriate for federal privacy legislation to impose different levels of responsibility on controllers and processors for achieving privacy outcomes. In particular, controllers, which determine the means and purposes of processing personal data, should have primary responsibility for satisfying legal privacy and security obligations. Controllers are the entities that, among other things, make decisions about consumers' data, including who it is shared with and how it is used.

On the other hand, processors, which handle data on behalf of the controller to implement the controller's objectives, should be responsible for securing the personal data they maintain and following the instructions pursuant to their agreements with relevant controllers. The processor/controller distinction provides organizations with a clear picture of their respective legal obligations, while still ensuring consumers are protected.

Importantly, adopting a distinction between controllers and processors and their levels of responsibility would promote interoperability among privacy frameworks and consistency in multinational, business-to-business contracts and other arrangements. The distinction is fundamental to privacy laws around the world, including the European Union's GDPR, and the many business relationships associated with global processing operations that have incorporated this distinction.

C. Provide Strong, Consistent Enforcement

Effective enforcement is important to protecting consumers' privacy, ensuring that organizations meet their commitments and legal obligations, and deterring potential violations. The FTC has demonstrated that it is highly capable of overseeing and enforcing those commitments and obligations, as is evident from the more than 100 privacy and data security enforcement actions the agency has brought under Section 5 of the FTC Act.[4] The FTC has also developed a deep understanding of the complexities of the digital economy. In addition, the FTC generally has observed the principle of bringing cases that remedy and deter harmful conduct, rather than punishing technical lapses. Given this strong record, the FTC should maintain its leadership role as the primary federal enforcer of consumer privacy protections under federal privacy legislation, and it should have the tools and resources necessary to carry out its mission effectively.

In addition, in order to provide consistent expectations for consumers and clear obligations for companies across the country, it would be appropriate for a strong federal law to replace, but not undermine the protections in, state laws. We recognize that states, such as California, have been leaders on this issue, passing laws aimed at enhancing consumer privacy protections. Importantly, the aim of a consistent national standard is not to weaken privacy protections provided by California or other state laws. Rather, the aim is to strengthen those laws by providing comprehensive, clear, and consistent protections for consumers across the country. Moreover, we believe that state attorneys general should continue to have the ability to enforce a strong, comprehensive federal privacy law. This will provide both better enforcement and a pathway for states to continue to promote and protect privacy.

[4] *See* FTC, *Privacy and Data Security Update* 2, 4 (2017).

III. The Path Forward

BSA members take their privacy commitments and obligations very seriously. At the same time, BSA members operate in a global environment that is increasingly complex in terms of technology, business and customer relationships, and regulation. A federal privacy law that sets strong standards and brings consistency to existing protections would help protect privacy, promote innovation, and contribute to U.S. leadership on privacy issues in the global marketplace. BSA strongly supports these goals, and we look forward to working with the Committee to achieve them.