Before the
DEPARTMENT OF COMMERCE
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
Washington, DC 20530

In the Matter of Developing the Administration's Approach to Consumer Privacy	))))	Docket No. 180821780-8780-01

COMMENTS OF BSA | THE SOFTWARE ALLIANCE

BSA | The Software Alliance
20 F Street, NW
Suite 800
Washington, DC 20001

November 9, 2018

TABLE OF CONTENTS

I. A Strong, User-Centric Consumer Privacy Framework Will Help Maintain Data-Driven Innovation and Global Data Flows. 2

A. The Importance of Personal Data to Innovation 3

B. The Importance of Global Data Flows 3

II. The Elements Of The Administration's Proposed Approach Align With BSA's Privacy Framework. 4

A. BSA Supports Strong Privacy Rights for Consumers. 5

B. Strong Transparency, Security, and Accountability Are Also Important to Protecting Consumer Privacy. 6

C. Businesses and Consumers Benefit from Clear Assignments of Data Protection Responsibilities and Consistency in Enforcement. 8

III. BSA Strongly Supports the Administration's High-Level Goals. 9

Before the
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
Washington, DC 20230

In the Matter of Developing the Administration's Approach to Consumer Privacy	))))	Docket No. 180821780-8780-01

COMMENTS OF BSA | THE SOFTWARE ALLIANCE

BSA appreciates the opportunity to respond to the National Telecommunications and Information Administration's ("NTIA") Request for Comments on "Developing the Administration's Approach to Consumer Privacy" ("the RFC").[1] BSA encourages the NTIA and the Administration as a whole to pursue a consumer privacy approach that provides strong protections to consumers, recognizes the critical role that organizations' internal governance processes play in reaching consumer privacy protection goals, and provides for strong enforcement. If defined in a manner that provides companies with flexibility to determine how they implement protections, a privacy approach with these elements will protect consumer privacy interests and promote innovation and global data flows.

INTRODUCTION AND SUMMARY

BSA is the leading advocate for the global software industry. Our members are at the forefront of software-enabled innovation that is fueling global economic growth, including cloud computing and artificial intelligence ("AI") products and services. In the United States, software contributes $1.14 trillion to US GDP and supports 10.5 million jobs, with an impact in each of the 50 states and across a range of industries.[2] As global leaders in the development of data-driven products and services, BSA members prioritize the protection of consumers' personal data, and they understand that it is a key part of building consumer trust.

---

[1] Notice and Request for Comments, Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 48,600 (Sept. 26, 2018) ("RFC").

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

As the RFC recognizes, consumer trust is "at the core" of US consumer privacy policy.[3] Robust consumer privacy protections strengthen this trust and promote full participation in the digital economy. The Administration's proposed approach thoughtfully combines a focus on consumers and sound enforcement policy with the recognition of the complexity and many benefits of data processing in today's digital economy.

These comments proceed in three main parts. Part I discusses overarching considerations to help guide the Administration's deliberations on developing its consumer privacy approach. Part II offers comments on the Administration's proposed outcomes by providing further details about specific elements that BSA supports including in a consumer privacy framework. Many of the privacy outcomes that the Administration proposes are similar to the elements of BSA's Privacy Framework. Finally, Part III provides comments on the Administration's high-level goals. Notably, to achieve these goals, BSA supports federal consumer privacy legislation that establishes uniform federal standards, provides clear expectations for consumers, and sets clear obligations for businesses. Maintaining a nationally consistent set of strong consumer privacy standards is vitally important. Consumers expect consistent protections for personal data, whereas varying state and local standards create consumer confusion and impose significant compliance burdens on businesses, with little or no benefit to consumers. Although BSA supports a legislative solution, BSA also encourages the Administration to maintain its ongoing, multi-faceted efforts to advance consumer privacy protection and promote innovation.

I. A STRONG, USER-CENTRIC CONSUMER PRIVACY FRAMEWORK WILL HELP MAINTAIN DATA-DRIVEN INNOVATION AND GLOBAL DATA FLOWS.

Consumer privacy frameworks that provide sufficient flexibility, reasonable obligations, and interoperability with different privacy and data protection frameworks are critically important in the increasingly complex global environment in which BSA member companies operate. Such approaches promote consumer trust and support beneficial uses of data. They also can support global data flows, which are essential to fully realizing these benefits to consumers and the economy.

[3] RFC at 48,600.

A. THE IMPORTANCE OF PERSONAL DATA TO INNOVATION

Software-enabled technologies increasingly rely on data and, in some cases, personal data, to perform their intended functions. These data-driven advances are improving citizens' lives and creating economic benefits across multiple sectors of the economy. For example, AI technologies are providing myriad benefits to small and large businesses across a wide swath of industries, as well as consumers and society as a whole. AI is helping businesses solve complex, rapidly changing, global problems, including:

- **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."

- **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 incidents 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.

- **Education.** Educators use AI products to access the math resources they need in seconds, including lesson plans, activities, standards, and teaching strategies that allow them to customize material based on each student's abilities. These tools can help teachers be more efficient and enhance students' learning opportunities.

- **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.

B. THE IMPORTANCE OF GLOBAL DATA FLOWS

Maintaining global data flows is critically important to realizing many of the benefits of data-driven technologies like AI as well as developing and using cloud computing services to their maximum advantage. Global data flows enable multinational companies to scale global operations, startups to use cloud services to obtain digital infrastructure at lower costs, and small and medium-sized enterprises to use digital platforms to find customers and suppliers abroad.

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. Many businesses rely upon third-party retailers to sell their products and, therefore, need to move both customer and vendor data across borders to complete cross-border sales. And companies of all sizes benefit from cross-border data flows in the area of cybersecurity: When companies can transfer data freely across borders, they reap the full benefits of cloud computing through compartmentalized datasets that help prevent a breach in one location from infecting the full dataset.

As part of the dual goal of protecting privacy and spurring innovation, a privacy framework should not only recognize the importance of enabling legitimate uses of data where significant privacy risks have been mitigated or other operational controls have been put in place, but it also should facilitate cross-border data transfers while encouraging companies to implement accountable practices that ensure personal data will continue to be protected as it moves across borders.

II. THE ELEMENTS OF THE ADMINISTRATION'S PROPOSED APPROACH ALIGN WITH BSA'S PRIVACY FRAMEWORK.

BSA supports the Administration's proposed consumer privacy outcomes. The RFC's outcome-based framing is helpful because it puts the emphasis on the effectiveness of privacy protections and how they align with consumers' expectations, rather than on the specific means to achieve them. At the same time, some consideration of how these outcomes might be achieved in practice sheds light on possible routes and potential challenges to achieving specific outcomes. Last month, BSA released a Privacy Framework consisting of ten principles that brings all of these considerations together.[4] The Privacy Framework's elements provide a plan for strong consumer protections, strong organizational practices that support these protections, and consistent, robust enforcement.

[4] *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").

A. BSA Supports Strong Privacy Rights for Consumers.

Informed Choice. BSA agrees that sole reliance on notice and choice falls short of enabling consumers to make informed decisions about personal data collection and use in practice.[5] Other means also are important to consider in connection with achieving the underlying goal of affording consumers with appropriate control over personal data.

Still, in appropriate settings, consent has an important role to play, and BSA supports the principle of informed choice. If appropriately defined and implemented, informed choice would balance flexibility and certainty, while also meeting consumers' expectations. Two considerations are critical to striking this balance. First, 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. Second, 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. Organizations should obtain affirmative express consent from consumers when collecting this sensitive information.

Access, Correction, and Deletion. But, in light of the increasing challenges with consent—both with respect to understanding the implications of choices and the limited ability to implement them in settings where consent may be infeasible—other mechanisms to help consumers exercise greater control over their personal data also should be strengthened. In particular, providing consumers with the ability to access, obtain a copy of, correct, and delete personal data can add effectively to consumer control.[6] Organizations that determine the means and purposes of processing personal data should be primarily responsible for responding to these requests.

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 organization's services. To this end, consumers should be able to request information about whether organizations have personal

---

[5] *See* RFC at 48,601 ("[T]he consent of an informed user is the end-goal of most approaches to consumer privacy, but in order to create legal clarity, this principle is implemented by mandating notice and choice. To date, such mandates have resulted primarily in long, legal, regulator-focused privacy policies and check boxes, which only help a very small number of users who choose to read these policies and make binary choices.").

[6] *See id.* at 48,602 ("Users should have qualified access [to] personal data that they have provided, and to rectify, complete, amend, or delete this data.).

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.

The ability to request a copy of, access, correct, or delete personal data must fall within certain limits. 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. STRONG TRANSPARENCY, SECURITY, AND ACCOUNTABILITY ARE ALSO IMPORTANT TO PROTECTING CONSUMER PRIVACY.

Although giving consumers better ways to make informed choices about personal data and exercise control over it are vital to effective privacy protections, 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 transparency, security, and accountability in any consumer privacy approach.

Transparency. As suggested in the RFC, organizations should provide users of their services with clear and accessible explanations of their practices for handling personal data.[7] 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.

As the RFC notes, however, providing this information in a manner that is helpful to consumers can be challenging.[8] 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

[7] *See id.* at 48,601 (emphasizing that "[o]rganizations should take into account how the average user interacts with a product or service, and maximize the intuitiveness of how it conveys information to users").

[8] *See id.* (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).

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 as defaults into a privacy approach. In particular, BSA recommends building a transparency principle or outcome around the following specific elements: (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.

Security. Data security is integral to many BSA members' business models and how they safeguard valuable data assets, including those of their customers. It is also integral to protecting personal data and privacy. Organizations should 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. In addition to these considerations, which the Administration's proposed outcome embraces,[9] a data security principle or outcome 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 based on 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)

[9] *See id.* at 48,601-48,602 (recommending that organizations adopt "reasonable security measures appropriate to the level of risk associated with the improper loss of, or improper access to, the collected personal data; they should meet or ideally exceed current consensus best practices, where available").

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.

C. BUSINESSES AND CONSUMERS BENEFIT FROM CLEAR ASSIGNMENTS OF DATA PROTECTION RESPONSIBILITIES AND CONSISTENCY IN ENFORCEMENT.

Federal Trade Commission (FTC) Enforcement. Effective enforcement is important to protecting consumers' privacy, ensuring that organizations meet their commitments and legal obligations, and deterring potential violations. BSA members take their privacy commitments and obligations very seriously, and the FTC is highly capable of overseeing and enforcing those commitments and obligations. The FTC has brought approximately 100 privacy and data security enforcement actions under Section 5 of the FTC Act and hundreds more under narrower privacy statutes.[10] The FTC also generally has observed the principle of bringing cases that remedy and deter harmful conduct, rather than punishing technical lapses. Given this strong record, BSA agrees that the FTC should maintain its leadership role as the primary federal enforcer of consumer privacy protections and should have the tools and resources necessary to carry out its mission effectively.[11] To this end, BSA encourages the Administration to explore, in consultation with the FTC, how an organization's accountability measures should factor into both enforcement decisions and remedies.

Controller/Processor Distinction. 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 businesses that handle personal data to clearly define their responsibilities. The Administration should incorporate this distinction into its consumer privacy approach.

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

[11] *See* RFC at 48,602.

The Administration's approach also should recognize that it is appropriate 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. Processors should be responsible for following the instructions to which they agree 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 General Data Protection Regulation ("GDPR") and the many business relationships associated with global processing operations that have incorporated this distinction.

III. BSA STRONGLY SUPPORTS THE ADMINISTRATION'S HIGH-LEVEL GOALS.

In addition to supporting the Administration's proposed outcomes, BSA strongly supports the high-level goals that NTIA has articulated. Notably, BSA also supports federal legislation that would implement the privacy protections described in the RFC and outlined in BSA's Privacy Framework. We believe that a uniform federal law could provide clear expectations for consumers and clear obligations for businesses.

There are meaningful steps that the Administration can take in the absence of such legislation, and BSA supports the multi-faceted approach that the Administration is pursuing to achieve its goals. In general, a risk-based approach is essential to promoting innovation and protecting consumer privacy by keeping the focus of data protection efforts on outcomes, rather than unnecessarily imposing "cumbersome red tape" that often accompanies compliance-oriented frameworks.[12] Applying this risk-based approach comprehensively across all industries harmonizes domestic legal requirements, enables strong FTC enforcement, and facilitates global interoperability. It is essential to maintaining a system that accomplishes the dual goals of protecting privacy and spurring innovation.

[12] *See id.* at 48,602.

In addition, the Administration should continue to support current efforts parallel to the development of an overall consumer privacy approach. For example, BSA supports the National Institute of Standards and Technology's initiative to develop a voluntary enterprise risk management framework, which could lead to a useful operational tool that allows companies to strengthen privacy best practices. BSA also supports the Administration's important international advocacy efforts. Of particular importance are the Administration's ongoing efforts to discourage data localization measures. Data localization measures disrupt companies' operations and make it more costly to provide services in affected markets. Therefore, sustained engagement to prevent additional data localization measures – and the economic harm they cause in the countries that adopt them – is both warranted and consistent with the goal of interoperability. BSA also encourages the Administration to continue its efforts to facilitate cross-border data flows, particularly in connection with the EU-U.S. Privacy Shield and the Asia-Pacific Economic Cooperation's Cross-Border Privacy Rules ("CBPR") system. In this regard, BSA supports the FTC's enforcement of participating organizations' Privacy Shield and CBPR commitments, which helps to sustain the validity of such cross-border data transfer mechanisms.

The RFC, and much of the Administration's advocacy focus, appropriately recognize the impact of the development of a consumer privacy approach on US leadership abroad. In BSA's view, the elements of the BSA Privacy Framework—if applied globally—could enhance the delivery of innovative, data-driven products and services in countries around the globe.

As BSA highlighted in its comments to NTIA in July, the Administration should observe two key principles in its engagement abroad: (i) the Administration should seek commitments from foreign governments to refrain from adopting rules that force US enterprises to store data locally, or that otherwise limit their ability to transfer data across borders; and (ii) the Administration should urge foreign governments, when regulating activities relating to lawful online communications or commerce, to respect the limits of their jurisdiction and give due regard to US interests under established principles of international comity.[13]

[13] *See* BSA | The Software Alliance, Comments on International Internet Policy Priorities, NTIA Docket No. 180124068-8068-01, at 4-5 (July 17, 2018).

NTIA and other bureaus within the Department of Commerce should work closely with each other and other agencies and offices to implement these principles to help reduce barriers to cross-border data transfers. We look forward to discussing additional mechanisms that could be used to further this goal, particularly in connection with negotiations on digital trade with key trading partners.

* * * * *

The Administration's perspective is a critical part of the ongoing debate over consumer privacy. BSA would be pleased to serve as a resource to the Administration as it further develops its consumer privacy approach.

Respectfully submitted,

Shaundra Watson
Director, Policy
BSA | The Software Alliance
20 F Street, NW
Suite 800
Washington, DC 20001

November 9, 2018