



Before the
FEDERAL TRADE COMMISSION
Washington, DC 20580

In the Matter of)
Hearings on Competition and Consumer Protection in) Docket No. FTC-2018-0098
21st Century: Consumer Privacy)
)

COMMENTS OF BSA | THE SOFTWARE ALLIANCE
December 20, 2018

BSA | The Software Alliance appreciates the opportunity to provide these comments in connection with the Federal Trade Commission’s (“FTC”) upcoming public hearing on consumer privacy.¹ BSA is the leading advocate for the global software industry.² 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 U.S. GDP and supports 10.5 million jobs, with an impact in each of the 50 states and across a range of industries.³ 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 FTC, FTC Hearing on Competition and Consumer Protection in the 21st Century - February 2019, <https://www.ftc.gov/news-events/events-calendar/ftc-hearing-competition-consumer-protection-21st-century-february-2019> (last visited Dec. 10, 2018) (“Hearing Notice”).

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, Twilio, and Workday.

³ See Software.org: The BSA Foundation, *The Growing \$1 Trillion Economic Impact of Software*, at 5 (Sept. 2017), available at https://software.org/wp-content/uploads/2017_Software_Economic_Impact_Report.pdf. Consistent with the Commission’s instruction in its initial request for comments to disclose the source of “funding for research, analysis, or commentary that is included in a public comment,” we note that BSA contributes funding to Software.org: the BSA Foundation, which published the study cited here and the study cited in note 25, *Artificial Intelligence Maximizing the Benefits* (March 2018).

INTRODUCTION AND OVERVIEW

BSA agrees that changes in the technological and regulatory landscape since the FTC issued its comprehensive privacy report in 2012 make this a critical time for the FTC to “address[] fundamental questions about the goals of policymaking and enforcement in the privacy area.”⁴ The FTC has played a key role in promoting flexible, technology-neutral, risk-based privacy and security frameworks that are best suited to protect consumer data in a dynamic marketplace. BSA appreciates that the Commission and its staff recently called for Congress to consider federal privacy legislation; we also support federal privacy legislation that establishes uniform national standards, provides clear expectations for consumers, and sets clear obligations for businesses.⁵ Nationwide privacy and data security standards are critical to prevent varying state and local standards, which create consumer confusion and impose significant compliance burdens on businesses, with little or no benefit to consumers. Although legislation would most directly advance the United States toward the goals of “seamlessly” protecting consumers’ privacy interests while “provid[ing] greater clarity to businesses” and “retaining the flexibility required to foster competition and innovation,”⁶ BSA also encourages the FTC to continue using its existing authority to advance a “flexible, risk-based approach to consumer privacy”⁷ through enforcement, business guidance, and consumer education.

In addition to conducting its own comprehensive examination of consumer privacy, the FTC should remain engaged with parallel efforts within the Administration. 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 efforts to develop a consumer privacy approach as well as its important international advocacy efforts, particularly in

⁴ See Hearing Notice, *supra* note 1.

⁵ See Statement of the FTC on *Oversight of the Federal Trade Commission: Hearing Before the Subcomm. on Consumer Protection, Product Safety, Insurance, and Data Security, S. Comm. on Commerce*, at 10 (Nov. 27, 2018) (“FTC Testimony”); Comments of FTC Staff on Developing the Administration’s Approach to Consumer Privacy (Nov. 9, 2018), NTIA Docket No. 180821780-8780-01, at 20-21 (“FTC Staff Comments”).

⁶ FTC Testimony, *supra* note 5, at 10.

⁷ FTC Staff Comments, *supra* note 5, at 3.

connection with the EU-U.S. Privacy Shield and the Asia-Pacific Economic Cooperation's Cross-Border Privacy Rules ("CBPR") system. The FTC plays a vital role in these frameworks by enforcing participating organizations' Privacy Shield and CBPR commitments, which helps to sustain the validity of such cross-border data transfer mechanisms. Consistency between the FTC and the Administration will also be helpful to businesses that seek to implement guidance that results from these efforts, as well as discussions of federal privacy legislation.

These comments address two sets of issues raised in the FTC's notice of its February 2019 privacy hearing. Part I provides comment on specific elements of a comprehensive consumer privacy framework and discusses how to incorporate these elements into a flexible, risk-based approach. Part II responds to the Commission's questions concerning automated decisionmaking, emphasizing that data plays an essential role in realizing the tremendous economic growth and breakthroughs on vexing social challenges that AI can deliver. BSA members are attuned to the possible risks associated with certain applications of AI, but it is essential for the FTC and all stakeholders to develop privacy frameworks that take account of AI's complexity and a realistic picture of its risks and benefits.

I. The FTC Should Continue to Promote a Consumer Privacy Framework That Provides Strong Protections Through a Flexible, User-Centric Approach.

BSA supports federal legislation implementing best practices that increase the transparency of personal data collection and use; enable and respect informed choices by providing governance over that collection and use; provide consumers with control over their personal data; provide robust security; and promote the use of data for legitimate business purposes. The same objectives should govern *any* consumer privacy framework, legislative or otherwise. BSA's Privacy Framework articulates ten principles that outline a general plan for strong consumer protections; strong organizational practices that support these protections; and consistent, robust enforcement.⁸ These principles can help inform the development of specific elements in a framework that protects consumer privacy and promotes innovation.

⁸ 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"). In addition to the specific bullets referenced in this submission that were under the "General Questions" section in the Hearing Notice, we also address issues raised in the "Questions About Legal Frameworks."

A. Sensitivity-Based Privacy Protections⁹

BSA supports maintaining a sensitivity-based privacy framework, in which the type of personal data is part of what determines which privacy protections and obligations should apply to the data. Such a framework helps 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. Categories of personal data types that BSA recommends classifying 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.

B. Targeting Privacy Interventions (Transparency and Choice Mechanisms)¹⁰

Any privacy framework must provide sufficient flexibility for companies to inform consumers of their data practices and, where choices are appropriate, provide them in a manner that is helpful to consumers and supports the aim of giving them more control over their personal data. Although sole reliance on notice and choice falls short of enabling such decisions in practice, BSA encourages the FTC to view transparency and choice as tools that, if used appropriately, enable effective consumer control over personal data.

Transparency is an important element of consumer privacy protection. Organizations should 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. 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

⁹ This section addresses questions in the fourth bullet point under "General Questions" in the Hearing Notice.

¹⁰ This section addresses questions in the seventh bullet point under "General Questions" in the Hearing Notice.

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 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.

In certain settings, consent has an important role to play in providing consumers with appropriate control over personal data, 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, as discussed above. Organizations should obtain affirmative express consent from consumers when collecting sensitive personal data.

The FTC also should consider other means of providing consumers with control over their data, given that choices are growing in complexity for consumers, and there are settings in which consent may be infeasible. In particular, providing consumers with the ability to access, obtain a copy of, correct, and delete personal data can add effectively to consumer control. To this end, 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. Organizations that determine the means and purposes of processing personal data should be primarily responsible for responding to these requests.

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.

C. Improving Accountability¹¹

Accountability within organizations that handle personal information is also critical to effective data protection. The central objective of 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 identifying 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 – such as data protection impact assessments – should not be mandatory. Instead, a privacy framework should focus on the objectives of responsible data processing. Impact assessments may help some organizations to achieve this end, but there is too much variability in organizations' resources and data processing operations to justify imposing such an across-the-board requirement for all data processing.

¹¹ This section addresses questions in the eighth bullet point under "General Questions" in the Hearing Notice.

D. Deidentification¹²

The three-part standard for deidentification that the FTC articulated in 2012 has played a useful and positive role in shaping data protections and enabling beneficial data use over the past several years.¹³ In addition to striking a practical balance of technical, administrative, and contractual measures,¹⁴ the FTC's deidentification standard encourages reasonable, risk-reducing privacy protections that preserve opportunities for innovation.¹⁵ Importantly, the FTC also declared that data that is deidentified in accordance with the standard "will fall outside the scope of the framework" set forth in its 2012 privacy report.¹⁶

BSA encourages the FTC to maintain its overall approach toward deidentification. In particular, contractual controls, technical privacy and security controls, or an appropriate combination of them should be the touchstone of any approach to deidentified data. In addition, it is appropriate to exempt such data from most or all obligations of a privacy framework. The use of deidentified data significantly reduces privacy risks to individuals, so there is little justification to subject appropriately deidentified data accompanied by reasonable controls to the full set of privacy obligations. Moreover, devising, implementing, and monitoring appropriate deidentification methods may require significant resources; deeming deidentified data to be partially or entirely outside the scope of a privacy framework would provide an incentive for organizations to commit resources to deidentification in the first place.

E. Competition on Privacy and Security¹⁷

Data security is integral to protecting privacy. It is also central to many BSA members' business models and how they safeguard valuable data assets, including those of their customers. In this regard, data security is a basis of competition in its own right and as an enabler of privacy protections.

¹² This section addresses questions in the fifteenth bullet point under "General Questions" in the Hearing Notice.

¹³ See FTC, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* 21-22 (2012) [hereinafter "FTC Privacy Report"].

¹⁴ See *id.*

¹⁵ See *id.* at 21 (noting that the technological measures standard "is not an absolute one; rather, companies must take reasonable steps to ensure that data is de-identified").

¹⁶ *Id.* at 22.

¹⁷ This section addresses questions in the thirteenth bullet point under "General Questions."

As BSA highlighted in its initial comments on Hearing Topic 2,¹⁸ security is a hallmark of cloud computing services that many BSA members provide. Providers of cloud-based systems use their expertise and ever-advancing threat detection and risk management to protect against cyberattacks through state-of-the-art, multilayered defense-in-depth measures deployed across their systems. Businesses benefit from this protection, as do the individuals whose data is involved.

Cloud providers are better positioned to provide enhanced security for several reasons. Cloud providers can invest more in building and managing their security infrastructure than any individual company that manages their own software and systems; they have a level of expertise and volume of staff dedicated to security that no individual customer can match; and they apply patches and updates to systems as the patches are released by vendors, while on premises customers often stay on old, unsecure patch sets to avoid business impact or disruption when they do it themselves. As a result, cloud providers are better equipped than individual companies to defend against individuals and criminal organizations seeking unauthorized access to data.

As software-enabled technologies become increasingly integrated into our daily lives and the basic functioning of our economy, the need to protect the security of personal information used by online services has become more than critical; it is indispensable. Data security is essential to maintaining consumer trust and enabling the data-driven services that underlie core functions of modern life and business. Any federal privacy law therefore needs to recognize the appropriate use of personal information for security purposes.

Addressing security threats requires a multi-faceted and holistic approach, beginning with industry efforts. BSA is a leader in this regard, and our members invest heavily in helping protect their customers, and society more broadly, against cybersecurity threats. For instance, BSA developed guiding principles that emphasize the importance of cybersecurity policy that is aligned with internationally recognized standards, risk-based, technology-neutral, outcome-focused, and flexible to

¹⁸ Comments of BSA | The Software Alliance on Topic 2: Competition and Consumer Protection Issues in Communication, Information, and Media Technology Networks, FTC Project No. P181201, at 5-6, *available at* <https://www.bsa.org/~media/Files/Policy/Data/08172018BSACommentsonFTCHearingsTopic2.pdf><https://www.bsa.org/~media/Files/Policy/Data/08172018BSACommentsonFTCHearingsTopic2.pdf>.

meet dynamic threats.¹⁹ BSA members are industry leaders in the development and adoption of security-by-design principles and secure software development lifecycle processes.²⁰ In addition, our members have played key roles in developing international standards, such as the ISO 27000 family of information security management standards that form the basis of the NIST *Framework for Improving Critical Infrastructure Cybersecurity*.

BSA appreciates the important role the FTC has played in encouraging companies to adopt sound security practices. For example, the FTC’s “Stick with Security” guidance provides useful, practical tips on the use of encryption, how to implement security-by-design, and the importance of following industry-driven standards. At the same time, the FTC’s guidance emphasizes flexibility, noting that a data security program should reflect the size of a business and the sensitivity of data it collects and maintains.

Still, more must be done to address the U.S. legal framework governing data security. 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. An unfortunate consequence of this uncertainty and complexity is that some companies may stop short of implementing certain advanced data security practices, simply because they cannot reconcile how the different sources of rules and guidance would treat the practices in question. To address these issues, federal privacy legislation should also establish a harmonized baseline data security standard. The law should recognize that 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, a data security standard 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

¹⁹ See BSA, *A Cybersecurity Agenda for the Connected Age*, available at https://www.bsa.org/~media/Files/Policy/BSA_2017CybersecurityAgenda.pdf.

²⁰ See *id.*

must be flexible, and they should be based on internationally recognized standards that also are risk-based, technology-neutral, and outcome-focused.

F. Fostering Accountability Among Third Parties²¹

The complex relationships that undergird much of the data-driven economy can present challenges when it comes to ensuring accountability. The essence of BSA's view of accountability is that an organization must fulfill its responsibilities with respect to personal data, irrespective of where or by whom the data is processed.

As a way of clarifying businesses' roles and responsibilities for handling personal data – and thus encouraging arrangements that foster accountability among third parties – BSA supports distinguishing 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. 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. The distinction is also fundamental to privacy laws around the world, including the European Union's General Data Protection Regulation and the many business relationships and accountability systems that businesses have developed to comply with these laws.

II. The Continuing Development of AI Technologies Depends on a Flexible, Balanced Privacy Framework.

AI technologies epitomize the rapid changes that have unfolded since the FTC last took a comprehensive look at consumer privacy issues, culminating in the Commission's 2012 Privacy Report.²² In the intervening years, nearly ubiquitous network connectivity, massive growth in the number of connected devices, and improvements in algorithms and analytical techniques have led to

²¹ This section addresses questions in the ninth bullet point under "General Questions" in the Hearing Notice.

²² See *generally* FTC Privacy Report, *supra* note 13.

dramatic, data-driven improvements in our ability to solve difficult societal challenges, bringing significant and widespread benefits. As BSA described in comments submitted to the FTC in August 2018, AI-based solutions are delivering myriad benefits to consumers and businesses in a wide and diverse variety of contexts, including improvements in healthcare, education, cybersecurity, and other areas.²³ To list just a few examples:²⁴

- **Fraud Detection.** AI is improving fraud detection by recognizing suspicious behavior and providing companies with real-time information that helps them identify and investigate different types of fraud, reducing the losses attributed to malicious actors by billions of dollars. These tools are also protecting 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 are helping enterprises stay ahead of their malicious adversaries.
- **Education.** Educators are using AI products to access the math resources they need in seconds, including lesson plans, activities, standards, information, and teaching strategies that allow them to customize material based on the student’s abilities.²⁵ These tools can help teachers be more efficient and enhance students’ education.
- **Inclusion.** AI is being used to promote inclusion. For example, AI systems, powered by data analytics, are at the heart of new devices and applications that can improve the lives of people with disabilities. For instance, AI is helping people with vision-related impairments interpret and understand visual content, such as photos and their physical surroundings. This technology opens new possibilities for people with vision impairments to navigate the world, giving them increased independence and greater ability to engage with their communities.

In addition to these more routine applications, AI makes possible other important tasks that would otherwise be economically or physically infeasible. For example, AI is used in submarines that map the ocean bed and measure ocean currents. And the future possibilities are endless. Flexible policy frameworks that spur data-driven innovation and do not impose unnecessary restrictions are vital to the

²³ See Comments of BSA | The Software Alliance on the Consumer Welfare Implications Associated with the Use of Algorithmic Decision Tools, Artificial Intelligence, and Predictive Analytics, FTC Project No. P181201, at 2-3, available at <https://www.bsa.org/~media/Files/Policy/Data/08172018BSACommentsonFTCHearingsTopic9.pdf>.

²⁴ See BSA, *Building Confidence and Trust in Artificial Intelligence Systems*, <https://ai.bsa.org/building-confidence-trust-in-artificial-intelligence-systems/>.

²⁵ See, e.g., Software.org: the BSA Foundation, *Artificial Intelligence Maximizing the Benefits* (March 2018), at 11, available at https://software.org/wp-content/uploads/AI_Report.pdf. See BSA funding disclosure, *supra* note 3.

continued development of these technologies.²⁶

Still, in some instances, stakeholders have inquired about the impact of predictive analytics and AI to support decision-making about consumers in certain areas, in part because of the challenges in understanding how the systems operate, and how they could potentially impact particular groups. These issues have led the FTC to inquire about the potential risk of unintended consequences of certain applications of AI. BSA and its members understand these risks and recognize the importance of increasing awareness of AI systems and providing meaningful information to enhance consumer understanding of these systems, particularly when such systems are deployed in contexts that affect consumers' eligibility in important areas, such as access to credit or housing.

BSA's members are proactively addressing these issues. Responsible technology innovation is a priority for BSA members, including efforts to develop AI technology with checkpoints for bias. Efforts to build consumer awareness, understanding, and trust are also critical as BSA's members proceed with their development of AI techniques. At the same time, research has shown that disclosing the algorithms, source code, or associated data sets is ineffective in helping to provide explanations, in part because they cannot be meaningfully understood in isolation. BSA therefore supports industry efforts to provide users of AI systems with the information necessary to instill confidence that such systems are operating as intended. Specifically, BSA has highlighted five key principles that could aid industry in facilitating increased understanding and promoting trust in the use of AI technologies: fairness; accuracy; data provenance; explainability; and responsibility.²⁷

Putting these principles into operation is an inherently context-specific exercise that must account for the wide variation in AI technologies and applications. BSA has highlighted practices that organizations may consider adopting to build trust and confidence in AI systems, including conducting

²⁶ See BSA, *AI Policy Overview*, http://www.bsa.org/~media/Files/Policy/BSA_2018_AI_PolicyOverview.pdf (identifying five pillars for facilitating responsible AI innovation: building confidence and trust in AI systems; sound data innovation policy; strengthened cybersecurity and privacy protections; investment in research and development; and workforce development). As part of its advocacy for sound data innovation policies, BSA has highlighted the need to (1) ensure data can move freely across borders; (2) facilitate open access to government data; (3) avoid the creation of new rights in business data; and (4) maintain predictable, technology-neutral competition policies. See BSA | The Software Alliance, *Spurring AI Innovation With Sound Data Policy*, https://ai.bsa.org/wp-content/uploads/2018/05/BSA_2018_AI_DataPolicy.pdf.

²⁷ See BSA | The Software Alliance, *Building Confidence and Trust in Artificial Intelligence Systems*, *supra* note 24.

in-house testing and evaluation of AI systems, ensuring a role for policy experts to assist computational scientists in the design and implementation phases, continuing monitoring after product release to detect and address unintended outcomes, and supporting continued research and analysis of transparent modeling.²⁸ While these practices will likely be applicable to a wide range of organizations, organizations should have the flexibility to determine which practices are appropriate for their uses of AI and how to implement them. As the FTC moves forward with its examination of automated decisionmaking and AI, BSA urges the Commission to recognize both the need for flexibility as well as the substantial, ongoing industry efforts to continue research in this complex area and to minimize the risks of AI while maximizing its benefits.

* * * * *

The FTC's hearing and broader re-examination of its consumer privacy framework come at a critical time and will provide a key forum for discussing the direction of U.S. consumer privacy law. BSA would be pleased to serve as a resource to the FTC as its assessment moves forward.

Respectfully submitted,

Shaundra Watson

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

²⁸ *See id.*