



**Competition and Consumer Protection in the 21st Century Hearings,
Project Number P181201**

**BSA | The Software Alliance Comments on Topic 2: Competition and Consumer
Protection Issues in Communication, Information, and
Media Technology Networks**

BSA | The Software Alliance (BSA) welcomes the opportunity to provide these comments in connection with the Federal Trade Commission’s (“FTC” or “Commission”) upcoming public hearings on competition and consumer protection in the 21st Century. The hearings promise to provide a valuable look at developments in the digital economy, and BSA applauds the Commission’s commitment to examining its policy and enforcement priorities in light of changes in technology, business models, and the international policy and legal environment.

BSA is the leading advocate for the global software industry before governments and in the international marketplace. 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.¹ 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.² Software, combined with the more than \$63 billion that the industry invests annually in research and development, serves as a powerful catalyst for U.S. economic growth, making companies more competitive and the economy more robust.

BSA’s comments focus on consumer protection issues in information networks and, in particular, the privacy and security issues implicated in this area.³ Our comments highlight two key issues. First, the near ubiquity of network connectivity and the massive growth in the number of connected devices have fueled data-driven innovations that are improving our ability to solve difficult societal challenges and bringing significant benefits to consumers. Second, consumer privacy and data security protections are integral to BSA

¹ BSA’s members include: Adobe, 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, Splunk, Symantec, Trend Micro, Trimble Solutions Corporation, and Workday.

² 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 to disclose the source of “funding for research, analysis, or commentary that is included in a public comment,” Request for Comments at 7, we note that BSA contributes funding to Software.org: the BSA Foundation, which published the study cited here and the study cited in note 7, *Artificial Intelligence Maximizing the Benefits* (March 2018).

³ See Fed. Trade Comm’n, Federal Trade Commission Announces Hearings on Competition and Consumer Protection in the 21st Century, at 3 (June 20, 2018) (“Request for Comments”). BSA is filing separate comments on hearing topic nine: the consumer welfare implications associated with the use of algorithmic decision tools, artificial intelligence, and predictive analytics. *Id.* at 5.

members' data-driven businesses. Maintaining strong personal data protections is an important priority for BSA member companies, and we encourage the FTC to continue its record of promoting the flexible, technology-neutral, risk-based privacy and security frameworks that are best suited to protect consumer data in a dynamic marketplace.

I. Data-Driven Innovation Is Benefitting Consumers and Companies Across the Economy

In the nearly 25 years since the FTC launched its first major study of consumer protection and competition policy in networked marketplaces,⁴ there have been profound changes in the ways that U.S. consumers live, shop, and work, and in how businesses operate. As one measure of these changes, electronic commerce sales as a share of all retail sales increased 36-fold from 1998 to 2015, from a share of 0.2 percent to 7.2 percent.⁵

Moreover, the nature of online business has changed and will continue to do so. Data is driving an increasing amount of economic activity in the U.S. and global economies. The decreasing costs of data storage, increasingly powerful networks, and the massive increase in the number of Internet-connected devices are all contributing to exponential growth in the amount of data traffic. Moreover, cloud computing services are providing secure, cost-effective, and scalable ways for companies to access and analyze this data, which is critical for AI and other data-driven techniques that empower consumers and workers, make businesses more agile and competitive, and boost the competitiveness and growth of the U.S. economy.

BSA members play key roles in providing the infrastructure for the data-driven economy. Many of our members primarily provide services to other enterprises, including data services that allow companies to leverage data to gain insight into their own operations and better meet their customers' needs, and cloud computing services, which provide security benefits and unprecedented efficiencies, including for small and medium-sized enterprises.

The increased use of data has provided immense economic and societal benefits. Below we highlight two areas –AI and cloud computing – that have undergone dramatic advances in recent years and have been integral to propelling the data-driven economy. These advances have taken place under flexible policy frameworks that spur data-driven innovation and do not impose unnecessary burdens. Maintaining this flexibility is vital to the continuing development of these technologies.

A. Artificial Intelligence Is Helping to Solve Significant Societal Challenges

AI technologies are providing myriad benefits to small and large businesses as well as consumers and society as a whole. Across a wide swath of industries, AI is helping businesses solve complex, rapidly changing, global problems. Below, we highlight a few examples of solutions based on AI.⁶

- **Fraud Detection.** AI is improving fraud detection by recognizing suspicious behavior and providing companies with real-time information that helps them identify and

⁴ See, e.g., Fed. Trade Comm'n, *Broadband Connectivity and Competition Policy* (staff report) (2007); Fed. Trade Comm'n, *Anticipating the 21st Century: Competition Policy in the New High-Tech Global Marketplace* (1996); Fed. Trade Comm'n, *Anticipating the 21st Century: Consumer Protection Policy in the New High-Tech Global Marketplace* (1996).

⁵ U.S. Dept. of Commerce, Economics and Statistics Admin., *New Insights on Retail E-Commerce* (June 26, 2017), <http://www.esa.doc.gov/reports/new-insights-retail-e-commerce>.

⁶ See BSA, *Building Confidence and Trust in Artificial Intelligence Systems*, <https://ai.bsa.org/building-confidence-trust-in-artificial-intelligence-systems/>.

investigate different types of fraud, reducing the losses attributed to malicious actors by billions of dollars.

- **Cybersecurity.** AI tools are revolutionizing how companies monitor network security, 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 cybersecurity tools are helping enterprises stay ahead of their sophisticated 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.⁷ These tools can help teachers be more efficient and enhance students' education.

B. Cloud Computing Delivers Significant Benefits to Consumers and Businesses

Cloud computing continues to revolutionize how consumers and businesses across all industry sectors use and benefit from computing. Cloud-based solutions provide access to flexible, scalable computing resources; real-time, worldwide access to data; greater reliability and backup of critical data; and easy integration of analytics and other software capabilities. All of these elements combine to make innovation and collaboration easier, more efficient, and more secure.

In fact, security is a hallmark of cloud services. 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.

The growth of cloud computing also has several far-reaching and significant economic impacts. For instance, cloud computing is a major force in driving IT investment. Demand for cloud computing accounted for 70 percent of market growth between 2012 and 2015 and is expected to represent 60 percent of growth through 2020.⁸

⁷ 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 2.

⁸ See BSA | The Software Alliance, *2018 BSA Global Cloud Computing Scorecard* (2018), at 1, available at http://cloudscorecard.bsa.org/2018/pdf/BSA_2018_Global_Cloud_Scorecard.pdf.

In addition, cloud computing's economic benefits ripple far beyond the immediate impact of making it more cost-effective for companies to obtain access to scalable computing resources. Cloud computing is democratizing access to advanced technologies, such as AI and data analytics.⁹ With the ability to use technologies that were previously only available to large organizations, small businesses are realizing gains in connectivity, productivity, and connectedness. And cloud computing fuels further advances in data analytics and AI by enabling companies to store, move, and analyze data in order to improve these techniques. The reduced cost to small businesses of accessing the same infrastructure in use by large enterprises, along with the enhanced capability to use advanced techniques to develop innovative products and services, contributes significantly to more robust competition in the marketplace.

II. Privacy and Data Security Are Key Consumer Protection Issues Relating to Information Networks

Customer trust in AI, cloud-based solutions, and other data-driven innovations is vital to ensuring their adoption and use across different industries. Realizing the full benefits of these innovations depends on, among other things, access to diverse data sets, and the ability to transfer that data across the globe at any time. In some situations, the data is non-personal, but in many instances, personal information is involved. As a result, privacy and data security protections are critical to the provision of data-driven services.

Ensuring the security, privacy, and integrity of the Internet ecosystem is a responsibility that businesses, private citizens, and the government share. BSA members are committed to improving privacy and security through their own practices as well as industry-driven software development and management best practices. The FTC will also continue to play an important role, by providing business guidance, actively promoting and participating in arrangements that promote cross-border data flows, and bringing enforcement actions under appropriate circumstances.

A. Consumer Privacy

BSA members care deeply about protecting individual privacy and recognize that appropriate protections for consumers' personal data are essential to realizing the benefits of data-driven services. Indeed, many BSA members' products and services, such as cloud computing, rely on customers' trust that valuable data, including personal information, will be kept secure.

In addition, companies regularly need to transfer personal data across borders for purposes that are both obvious to consumers, such as providing them the services that they request, as well as less apparent but still valuable, such as developing analytics to detect fraud and security threats. Using personal data in these beneficial ways carries with it the obligation to protect it.

BSA understands that, depending on the context, sensitive information, such as health information or financial information, may require heightened protections, and we support efforts to prioritize targeted enforcement efforts in areas that may lead to substantial harm. BSA also supports the implementation of best practices that increase the transparency of data collection and use; provide consumers with appropriate control over their personal information; enable and respect informed choices; provide reasonable security measures that appropriately address relevant risks; and promote responsible use of consumer data. Our member companies are at the forefront of data-driven innovation and have deep and

⁹ *Id.* at 5.

long-standing commitments to protecting consumers' personal data across technologies and business models.

The FTC also plays a key leadership role in protecting the privacy of consumers. Its thoughtful, deliberate approach to consumer privacy developed over a period in which the data-driven economy has grown dramatically larger and more complex. The Commission's sustained engagement with businesses and other stakeholders over time has enabled the Commission to stay up-to-date with developments in technology and business models and allowed companies to gain a better understanding of the FTC's privacy concerns.

In addition, the FTC has generally focused its enforcement efforts on privacy violations that cause the most significant harm to consumers. This approach has led to strong protections for consumers while also preserving an environment that encourages data-enabled innovation.

We encourage the Commission to continue its course of carefully examining changes in the marketplace, robust public engagement, and harm-based enforcement.

B. Security

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. Threat actors are becoming more sophisticated and determined, and companies constantly face attacks that aim to exploit or expropriate personal data, spread malware, or otherwise interfere with or commandeer network systems. Phishing, ransomware, and other types of attacks – particularly from automated, distributed threats such as malicious botnets – can lead to large-scale data theft and cause significant privacy violations. Data security is therefore essential to maintaining consumer trust and enabling the data-driven services that underlie core functions of modern life and business.

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 meet dynamic threats.¹⁰ BSA members are industry leaders in the development and adoption of security-by-design principles and secure software development lifecycle processes.¹¹ 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.

¹⁰ See BSA, *A Cybersecurity Agenda for the Connected Age*, available at https://bsacybersecurity.bsa.org/wp-content/uploads/2018/04/BSA_CybersecurityAgenda.pdf.

¹¹ See *id.*

Still, the FTC should consider the role it might play in further developing and promoting its guidance. 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. The FTC should consider ways in which it can help simplify these requirements – alone or with other agencies, and, crucially, in partnership with the industry stakeholders who are on the front lines of our defense against sophisticated cyber threats. We would look forward to serving as a resource to the FTC in this endeavor.

C. International Engagement on Privacy and Security Issues

Internet-enabled communications and commerce are borderless, which means that policies aimed at protecting consumers in a connected, data-driven economy must be crafted with a global lens. BSA welcomes the Commission's engagement on international consumer protection issues and appreciates its leadership in the global arena. In particular, BSA strongly supports policies that facilitate cross-border data transfers. The ability to move data freely across borders is critical for cloud computing, AI, and other emerging technologies that leverage real-time access to distributed data sets. As a result, privacy-preserving mechanisms that also facilitate these data flows are vital to the continued growth of the global economy.

Notably, the ability to transfer personal data from Europe is of critical importance to many companies, and the FTC is central to providing protections that enable transfers to the United States. For example, the EU-U.S. Privacy Shield Framework provides an important tool that facilitates transatlantic trade and protects individual privacy. The FTC's enforcement role is an integral part of the framework, as is its ongoing engagement with EU data protection authorities. In the recent House Energy and Commerce oversight hearing, the Commission reaffirmed its commitment to supporting the Privacy Shield.¹² In testimony before the Senate, BSA has also highlighted the importance of ensuring that transatlantic trade continues to thrive, and the important role the Privacy Shield plays in that effort.¹³ BSA appreciates the FTC's commitment and stands ready to assist in efforts to support the Privacy Shield, including by providing any relevant input about the software industry's privacy practices in connection with the upcoming annual review of the framework.

In addition, many companies rely on standard contractual clauses as the legal method to transfer data from the EU. They, too, are an important mechanism for ensuring seamless data transfers in a global economy, including, as referenced above, to aid in real-time analysis of potential security threats from around the globe. We encourage the Commission to continue its advocacy to support the availability and development of tools that facilitate cross-border data transfers, not only in the EU, but across the globe.

The FTC's work in the Asia-Pacific Economic Cooperation (APEC) is key to this effort. As the first economy to join the APEC Cross-Border Privacy Rules (CBPR) system, and the first enforcement agency to join the APEC Cross-Border Privacy Enforcement Arrangement,

¹² See Fed. Trade Comm'n, Prepared Statement Before the House of Representatives Committee on Energy and Commerce, Subcommittee on Digital Commerce and Consumer Protection (July 18, 2018), at 7 ("The Commission is committed to the success of the EU-U.S. Privacy Shield Framework, a critical tool for protecting privacy and enabling cross-border data flows.").

¹³ See Victoria Espinel, CEO, BSA, Testimony Before the Senate Committee on Commerce, Science, & Transportation Subcommittee on Communications, Technology, Innovation, and the Internet (Dec. 12, 2017), at 15, *available at* <http://www.bsa.org/~media/Files/Policy/Testimony/12122017BSAAITestimony.pdf>.

the U.S. government more broadly, and the FTC in particular, has demonstrated excellent leadership on this important initiative. We urge you to continue to support efforts to expand and otherwise enhance the utility of the system, including by promoting interoperability between the APEC CBPR system and data protection regimes of various regions, including the EU.

BSA also supports the fact-finding and analysis currently underway by the OECD's Working Party on Security and Privacy in the Digital Economy (SPDE). We appreciate U.S. leadership in the OECD and urge the FTC to work with other agencies to ensure that the United States promotes policy recommendations that are evidence-based, aligned with U.S. interests, and promote innovation. We understand that the OECD SPDE will initiate a review of the OECD's *Privacy Guidelines* later this year. The *Guidelines* have laid the foundation for the development of privacy laws around the world, while also reaffirming the importance of cross-border data flows. We urge the Commission to ensure that the OECD SPDE preserves the flexibility of the *Guidelines*, which promote continued innovation.

Finally, the FTC's bilateral engagement on privacy and security issues is increasingly important as countries consider developing and adopting new privacy laws and regulations. In particular, we appreciate your engagement in India as it develops its data protection framework and welcome your engagement in other emerging economies. Notably, a legislative proposal currently under consideration in India would implement data localization requirements, restrict cross-border data transfers, and otherwise potentially limit the use of data that could be leveraged to provide economic and societal benefits around the world. As countries develop new privacy laws, it is important to avoid fragmented approaches that create conflicting legal obligations, impose significant compliance burdens, or restrict the use and international transfer of data for organizations operating globally. The Commission's engagement with its global partners on these issues is an important part of a broader effort to guard against such fragmentation.

D. Harmonizing State and Federal Privacy and Security Regulations

BSA also supports the harmonization of state and federal privacy and data security laws. Harmonization at the federal level helps to avoid fragmented legal obligations, which in turn create complexity, unnecessary or even conflicting compliance burdens, and uncertainty for businesses. As one example, BSA has supported federal legislation that would include robust security requirements and provide a national standard that preempts the patchwork of varying state data breach notification obligations.¹⁴ In addition, as Congress continues its consideration of federal privacy legislation, an approach that harmonizes privacy and security obligations across the country, remains flexible to ensure continued innovation, and is sufficiently targeted to prevent significant consumer harm will be an important part of that effort.

¹⁴ See Aaron Cooper, Vice President, BSA, Testimony Before the House Committee on Financial Services Subcommittee on Financial Institutions and Consumer Credit, at 7-8 (Feb. 14, 2018), *available at* <http://www.bsa.org/~media/Files/Policy/Data/02142018BSATestimonyDataSecurityBreaches.pdf>.

III. Conclusion

BSA applauds the FTC's leadership on consumer privacy and data security issues, as well as its willingness to examine its role in light of changing technologies, business models, and policy challenges. As the Commission conducts its inquiry, we encourage you to consider the benefits to consumers, businesses, and governments of software-enabled, data-driven innovation and maintain policy frameworks that protect consumers from harmful privacy violations, promote adoption of appropriate security measures, and enable cross-border data flows. In so doing, the Commission will continue to fulfill its mission to protect consumers while also spurring innovation in the global online ecosystem. BSA would be pleased to provide the Commission with further information as its examination of privacy and security issues in information networks proceeds.