

Before the
DEPARTMENT OF COMMERCE
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
Washington, DC 20230

In the Matter of)
)
International Internet Policy Priorities) Docket No. 180124068-8068-01
)

COMMENTS OF THE
CONSUMER TECHNOLOGY ASSOCIATION

Julie M. Kearney
Vice President, Regulatory Affairs
Consumer Technology Association
1919 S. Eads Street
Arlington, VA 22202
(703) 907-7644

July 17, 2018

Table of Contents

Introduction and Summary1

I. The Free Flow Of Data Across Borders Promotes Innovation and Economic Growth3

II. The U.S. Government Should Continue to Foster Global, Industry-Wide, Consensus-Driven Privacy and Security Self-Regulation Around the World6

III. The U.S. Government Should Consistently Emphasize in International Discussions That the Benefits of Emerging Technologies and Trends Weigh Against Premature Regulatory Action9

Conclusion11

Before the
DEPARTMENT OF COMMERCE
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
Washington, DC 20230

In the Matter of)
)
International Internet Policy Priorities) Docket No. 180124068-8068-01
)

THE CONSUMER TECHNOLOGY ASSOCIATION

The Consumer Technology Association (“CTA”)¹ respectfully submits these comments for consideration by the National Telecommunications and Information Administration (“NTIA”) in response to its Notice of Inquiry on International Internet Policy Priorities (“NOI”).² CTA encourages NTIA to continue its efforts to promote growth and innovation for the internet and the internet-enabled economy.

INTRODUCTION AND SUMMARY

CTA represents an industry that supports more than 15 million U.S. jobs and generates more than \$351 billion in revenue in the United States. CTA also produces CES[®], which serves as the global stage for innovation; it has been a proving ground for innovators and breakthrough technologies for more than fifty years. Each year, CES[®] showcases the dynamic nature of technology and the consumer benefits that are possible when companies innovate freely. CES[®]

¹ The Consumer Technology Association (“CTA”)TM is the trade association representing the \$351 billion U.S. consumer technology industry, which supports more than 15 million U.S. jobs. More than 2,200 companies – 80 percent are small businesses and startups; others are among the world’s best known brands – enjoy the benefits of CTA membership including policy advocacy, market research, technical education, industry promotion, standards development and the fostering of business and strategic relationships. CTA also owns and produces CES[®] – the world’s gathering place for all who thrive on the business of consumer technologies. Profits from CES are reinvested into CTA’s industry services

² NTIA, *International Internet Policy Priorities*, Notice of Inquiry, 83 Fed. Reg. 26,036 (June 25, 2018) (“NOI”)

2018 demonstrated the proliferation of smart, connected devices available today, and the ongoing advances artificial intelligence (“AI”) and other emerging technologies are sure to continue to make their mark at CES[®] and beyond.

Advances in internet technologies – such as the Internet of Things (“IoT”) – combined with innovation-friendly policies can help the U.S. maintain economic growth and its global leadership role in technology.³ Moreover, innovation-friendly policies at home and abroad can help to unleash economic development and create consumer benefits around the world. This is particularly critical in markets for early-stage technologies like the IoT and AI, for which the full scope of potential uses is just beginning to come into view.

As NTIA fulfills its statutory role as the President’s “principal adviser on telecommunications policy pertaining to the Nation’s economic and technological advancement,”⁴ coordinates with other federal agencies, and interacts with its foreign counterparts, it should continue to champion the policies and principles that have allowed the internet ecosystem to flourish, and that will allow the next phases of internet innovation thrive as well. Specifically, these policies and principles include:

- *Free Flow of Information:* The free flow of data enables companies of all sizes to source, sell, and compete in the global marketplace. Data localization requirements and other barriers to digital trade are inimical to this system.

³ See Comments of the Consumer Technology Association, The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things, Docket No. 170105023-7023-01 (filed Mar. 13, 2017) (“CTA IoT Green Paper Comments”); Comments of the Consumer Technology Association f/k/a the Consumer Electronics Association, The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things, Docket No. 1603311306-6306-01 (filed June 2, 2016); see also Consumer Technology Association, Internet of Things: A Framework for the Next Administration (Nov. 2016), <http://www.cta.tech/cta/media/policyImages/policyPDFs/CTA-Internet-of-ThingsA-Framework-for-the-Next-Administration.pdf>.

⁴ 47 U.S.C. § 902(b)(2)(D).

- *Privacy and Security:* Voluntary, consensus-based, global standards and best practices are the best approach to improving privacy and security. They address privacy and security issues as they emerge, provide the flexibility to innovate, and better enable companies to provide products and services in the global marketplace.
- *Emerging Technologies and Trends:* Emerging technologies and trends, including AI, have the potential to make a significant impact on our world. NTIA should advocate both at home and abroad for flexible, technology-neutral policies and against unwarranted regulatory intervention. Prescriptive and premature regulation, however well-intentioned, could inhibit the development and deployment of innovative technologies that can generate economic growth and improve consumers' lives.

I. THE FREE FLOW OF DATA ACROSS BORDERS PROMOTES INNOVATION AND ECONOMIC GROWTH

NTIA should continue to promote cross-border data flows and other arrangements that facilitate innovation and economic growth.⁵ U.S. policy that focuses on enabling the free flow of data across borders creates opportunities for all businesses – large companies, but also small businesses and workers in all industries – to reach global markets. U.S. innovation, economic growth, advanced manufacturing and job creation depend on American companies' ability to easily access new markets abroad – and the ability of American companies to access new markets abroad depends directly on their ability to easily transfer data to and from such markets.

The economic stakes of cross-border data flows are enormous. According to CTA's *U.S. Economic Contribution of the Consumer Technology Sector Report*, U.S. tech exports generated \$379 billion, or 17 percent of total U.S. exports, in 2015.⁶ As CTA previously explained to the Office of the United States Trade Representative,

Over the last decade, the Internet has created new opportunities for cross-border trade and investment, enabling small businesses around the world

⁵ See NOI at 26038 (asking about what role NTIA can play in reducing restrictions to the free flow of information).

⁶ CTA, *U.S. Economic Contribution of the Consumer Technology Sector Report*, at E-2 (Aug. 2016), available at <http://www.cta.tech/cta/media/ResearchImages/U-S-Economic-Contribution-of-the-Consumer-Technology-Sector-2016.pdf>.

to connect with customers and suppliers in the global market without building their own multinational supply chains.... It is clear that digital trade and e-commerce have become important for multinational companies and small and medium-sized businesses alike to market their products or services in the global marketplace.⁷

It is therefore appropriate that NTIA has identified the free flow of information as an international internet policy priority, and CTA encourages NTIA to continue to focus on it.⁸

In particular, the United States must resist protectionism, which can arise through restrictions on data flows and certain forms of liability for internet companies, among other things. Trade agreements are one vehicle that the United States can use to discourage data localization laws and provide appropriate liability protections. To this end, the United States should work toward ensuring that trade agreements include provisions that address cross-border data flows, fair use and intermediary liability protections and promote international harmonization of standards and regulations.⁹ To the extent that NTIA has a role in developing the administration's position in such discussions, it should advocate for provisions that support a global, open internet and protect cross-border data flows.

Data localization laws in particular are a troubling trend. Protecting privacy, civil liberties, or national security is often cited as justifications for these laws,¹⁰ but often they have the opposite effect. Rather than protect individuals and their information, data localization laws

⁷ CTA, Letter to Edward Gresser, Office of the United States Trade Representative, at 3 (June 12, 2017), <http://www.cta.tech/cta/media/policyImages/policyPDFs/CTA-NAFTA-Comments.pdf> (“CTA USTR Letter”).

⁸ NOI at 26,037 (noting that “[t]he free flow of information is critical not only to the protection of free speech online, but to the continued growth of the global economy.”).

⁹ See USTR, *Key Barriers to Digital Trade*, Mar. 2017, <https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2017/march/key-barriers-digital-trade> (citing data localization, web filtering, and other barriers to digital trade); see also CTA USTR Letter at 2-4, 7-8 (urging protection of cross-border data flow, internet intermediaries, and intellectual property rights in trade negotiations).

¹⁰ See NOI at 26,037 (noting that certain governments are increasingly imposing restrictions on the free movement of data and often for reasons such as domestic surveillance or protectionism).

can undermine information privacy and security, information accuracy, and civil liberties.¹¹ Moreover, they disrupt data flows, force providers of online services to deploy inefficient systems and operations, and add significant costs and burdens. In turn, data localization laws can threaten the ability to provide such services altogether, particularly of startups and other businesses that may be unable to shoulder the added costs.

Ensuring intermediary protections is another key way to protect the free flow of information and internet-enabled trade. Many business models work because intermediaries can host online transactions without being held liable for the vast amounts of content surrounding each transaction. Specifically, intermediary liability laws like Section 230 of the Communications Decency Act enable internet services to host, process, and distribute user-generated content without being treated as the creator or originator of such content for purposes of determining liability.¹² Clear and predictable liability protections like Section 230 are needed to protect and ensure the free flow of information and the digital trade it enables.

NTIA and the administration as a whole also have a critical role to play in ensuring that data protection laws do not become trade barriers.¹³ Arrangements such as the EU-U.S. Privacy Shield and APEC Cross-Border Privacy Rules enable cross-border data flows by ensuring consistent, robust data protections, while also offering flexibility to companies that must operate

¹¹ See, e.g., Bret Cohen, Britanie Hall, and Charlie Wood, *Data Localization Laws and Their Impact on Privacy, Data Security and the Global Economy*, Antitrust Vol. 32, No. 1 (Fall 2017), available at https://www.americanbar.org/content/dam/aba/publications/antitrust_magazine/anti_fall2017_cohen.auth_checkdam.pdf; Erica Fraser, *Data Localization and the Balkanisation of the Internet*, SCRIPTed Vol. 13, No. 3 (Dec. 2016), available at <https://script-ed.org/wp-content/uploads/2016/12/13-3-fraser.pdf>; Josephine Wolff, *Borders in the Cloud*, Slate (Nov. 20, 2017), http://www.slate.com/articles/technology/future_tense/2017/11/countries_are_increasingly_imposing_borders_on_the_cloud.html.

¹² See 47 U.S.C. § 230(c).

¹³ See NOI at 26,037-38 (noting NTIA's work on the EU-U.S. Privacy Shield and APEC Cross-Border Rules).

under different legal regimes. CTA therefore encourages NTIA to continue its work in support of these data transfer mechanisms.

II. THE U.S. GOVERNMENT SHOULD CONTINUE TO FOSTER GLOBAL, INDUSTRY-WIDE, CONSENSUS-DRIVEN PRIVACY AND SECURITY SELF-REGULATION AROUND THE WORLD

A lesson learned from experience with the internet economy is that consistent, effective privacy and security protections – two of the foundations of consumer trust – are most likely to develop when governments themselves take a holistic, technology-neutral, and business model-neutral view of privacy and security risks. Under this policy principle, global, industry-wide, consensus-based standards and best practices have become a key element of protecting privacy and security on the internet. Self-regulatory and other industry-driven, consensus-based approaches not only address issues posed by rapidly evolving technologies but also lead to globally harmonized requirements, thereby accelerating adoption, driving competition, and enabling cost-effective introduction of new technologies. And such approaches help keep protections up-to-date, including the development of risk-based approaches to privacy and security, security by design, the ability to patch insecure software and devices, and the use of strong encryption.

NTIA should work with its fellow agencies to continue to foster voluntary, industry-driven global technical standards and self-regulatory approaches within the federal government and in international fora.¹⁴ In this regard, CTA appreciates and supports the work of NTIA and the National Institute of Standards and Technology (“NIST”) to encourage private sector leadership on privacy and security issues. CTA supports, for example, the various

¹⁴ See, e.g., NISTIR 8200 (recommending that “agencies should *work with industry* to initiate new standards projects in Standards Developing Organizations”) (emphasis added).

multistakeholder processes conducted by NTIA¹⁵ and NIST's partnership with industry to develop and improve the Cybersecurity Framework.¹⁶ Likewise, CTA supports the ongoing process led by the Departments of Commerce and Homeland Security under Executive Order 13800 to promote industry and government stakeholder action to strengthen U.S. cybersecurity by addressing botnets and other automated, distributed threats.¹⁷

These kinds of frameworks give the private sector the incentive to develop more specific and effective standards and practices, including those that are interoperable across the world, and CTA and its members are at the forefront of proactively addressing emerging IoT privacy and security concerns. For instance, in early 2015, CTA began a process to establish a first-of-its-kind set of voluntary guidelines for private sector organizations that handle personal wellness data, which often is generated by wearable technologies. The process culminated in CTA's October 2015 announcement of the *Guiding Principles on the Privacy and Security of Personal Wellness Data*, which establish a baseline, voluntary framework to promote consumer trust in

¹⁵ See, e.g., Cybersecurity Vulnerabilities, available at <https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities>; Internet of Things (IoT) Security Upgradability and Patching, available at <https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security>; Software Component Transparency, available at <https://www.ntia.doc.gov/SoftwareTransparency>; see also CTA IoT Green Paper Comments at 10-11 ("NTIA appropriately has used its multistakeholder processes to further catalyze industry discussion on cybersecurity-related issues, with the stated goal of achieving consensus-based positive outcomes.").

¹⁶ See, e.g., Comments of the Consumer Technology Association, Proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity, at 1-2 (filed Apr. 10, 2017) ("CTA appreciates the opportunity provided by NIST for industry to continue driving the development of the Framework in a manner that protects American citizens and infrastructure by promoting business and entrepreneurial flexibility to deploy new technologies and risk management solutions tailored to companies' individual cybersecurity needs.").

¹⁷ See Press Release, Consumer Technology Association, *Public-Private Partnerships Critical to Fighting Cyber Treats, Says CTA*, May 30, 2018, available at <https://www.cta.tech/News/Press-Releases/2018/May/Public-Private-Partnerships-Critical-to-Fighting-C.aspx>.

technology companies.¹⁸ The *Guiding Principles* offer an example of how industry can address to issues raised by new technology far more nimbly than regulations could.

In addition, in conjunction with the administration's efforts to improve cybersecurity across the internet ecosystem in collaboration with the industry, CTA is actively undertaking efforts to develop meaningful progress in IoT device security. In May 2018, CTA announced that it is working with the Council to Secure the Digital Economy to develop an International Anti-Botnet Guide that will advance best practices across all the components of the internet ecosystem to address automated, distributed threats that harness unsecured devices for malicious purposes.¹⁹ To bolster this internet ecosystem-wide effort, CTA has convened a group of cybersecurity experts to fight botnets and other security threats to consumer technologies by organizing and increasing the visibility of the large body of available standards, best practices, secure ecosystems and third-party security certification programs. These efforts to reach all corners of the IoT ecosystem illustrate the coordinated, cross-industry and global approach that is necessary to address inherently international internet security issues.

¹⁸ See Press Release, Consumer Electronics Association, *Association Unveils First-of-Its-Kind, Industry Supported Principles on Wellness Data Privacy*, Oct. 26, 2015, available at <https://www.cta.tech/News/Press-Releases/2015/October/Association-Unveils-First-of-Its-Kind,-Industry-Su.aspx>.

¹⁹ See Press Release, Council to Secure the Digital Economy, *CSDE Adds CTA as Strategic Partner on International Anti-Botnet Guide*, May 30, 2018, available at <https://www.ustelecom.org/news/press-release/csde-adds-cta-strategic-partner-international-anti-botnet-guide-0>.

III. THE U.S. GOVERNMENT SHOULD CONSISTENTLY EMPHASIZE IN INTERNATIONAL DISCUSSIONS THAT THE BENEFITS OF EMERGING TECHNOLOGIES AND TRENDS WEIGH AGAINST PREMATURE REGULATORY ACTION

The primary goal of U.S. government policy on emerging technologies should be to promote innovation. Accordingly, as NTIA engages with its counterparts abroad, it should emphasize the potential benefits of emerging technologies, rather than allow discussions to focus primarily on the risks, which can all too easily turn into regulations that purport to protect consumers from hypothetical dangers. Moreover, the U.S. should encourage advocate the principle that any regulation of emerging technologies should be narrowly targeted to address a specific, concrete harm.

Substantial consumer benefits from IoT technology could be lost if IoT discussions focus disproportionately on risk. Consumers understand that data from the smart technologies they use make possible the far-reaching benefits of the connected world. For example, wearable health monitors, connected cars, and smart energy meters, and the data that they create, process, and share, have profoundly improved consumers' ability to make choices that improve their lives and bring broader benefits to society. Policymakers should not simply assume that consumers do not understand these technologies and thus require regulatory interventions to "protect" them.

AI is another set of technologies about which the government can help increase consumer trust. AI has the potential to transform economies, industries and our everyday lives, improving everything from healthcare to cybersecurity,²⁰ and could contribute over \$15 trillion to world

²⁰ See Gary Shapiro, *Who's afraid of artificial intelligence? It could solve many of our nation's most difficult issues*, Fox News, May 8, 2018, <http://www.foxnews.com/opinion/2018/05/08/whos-afraid-artificial-intelligence-it-could-solve-many-our-nations-most-difficult-issues.html>; see also Gary Shapiro, *Harnessing the Power of Artificial Intelligence*, xconomy, Mar, 16, 2018, <https://www.xconomy.com/boston/2018/03/16/harnessing-the-power-of-artificial-intelligence/>.

economy by 2030.²¹ Despite these immense potential benefits, CTA research has found that public trust is one of the three main barriers to development and implementation of AI,²² and AI has created concerns about the effects it will have on our workforce.²³ Again, private sector-led efforts offer the best prospect of identifying and addressing the underlying concerns.

Accordingly, CTA recently launched an AI working group that includes representatives of companies that are leading AI development and deployment and understand AI's great potential as well as its risks. CTA has sought to address AI's workforce challenges head-on, including through the creation of CTA's 21st Century Workforce Council.²⁴ The Council serves as a leadership forum to address the nation's skills gap, ensure the U.S. tech sector has the high-skilled workers it needs, and devise strategies to upskill U.S. workers to succeed in the 21st century. Collaboration between industry and government could help advance these solutions far more effectively than preventative over-regulation.

NTIA should also work with other federal agencies to counter broader policies that focus disproportionately on the risks of emerging technologies. For instance, the ePrivacy Regulation being developed in the European Union could impose unwarranted and unrealistic burdens on IoT devices and data-driven services,²⁵ and protectionist trade policies could put a damper on the

²¹ PwC, *Sizing the prize*, <https://www.pwc.com/gx/en/issues/data-and-analytics/publications/artificial-intelligence-study.html>

²² See CTA, *Current and Future Prospects of Artificial Intelligence*, Mar. 2018, <https://www.cta.tech/Research-Standards/Reports-Studies/Studies/2018/Current-and-future-prospects-of-Artificial-Intelli.aspx>.

²³ See Testimony of Gary Shapiro, Before the House Oversight Committee, Subcommittee on Information Technology hearing- "*Game Changers: Artificial Intelligence Part III, Artificial Intelligence and Public Policy*," Apr. 18, 2018, available at <https://oversight.house.gov/wp-content/uploads/2018/04/Shapiro-CTA-Statement-AI-III-4-18.pdf> ("Shapiro AI Testimony").

²⁴ See *id.*

²⁵ See, e.g., Nick Wallace, *EU e-Privacy Proposal Risks Breaking 'Internet of Things'*, EUOBSERVER, May 22, 2018, <https://euobserver.com/digital/141302>.

global supply network for critical technology components, unnecessarily driving up the cost of AI-powered goods.²⁶ NTIA should emphasize within the federal government and to its counterparts abroad how inflexible and/or technology-specific laws, regulations, and policies can slow the development and deployment of emerging technologies, in turn reducing and delaying the benefits and economic growth these technologies will bring.

CONCLUSION

CTA appreciates NTIA's past and current efforts to promote a global, open internet that supports U.S. jobs and economic growth. Although the internet policy issues that companies face in the international arena are growing in economic significance and complexity, market-driven solutions and private sector leadership remain the best means to promote growth and innovation. CTA encourages NTIA to continue to keep this principle in the foreground of its international internet policy engagements.

Respectfully submitted,

CONSUMER TECHNOLOGY
ASSOCIATION

By: /s/ Julie M. Kearney

Julie M. Kearney
Vice President, Regulatory Affairs
1919 S. Eads Street
Arlington, VA 22202
(703) 907-7644

July 17, 2018

²⁶ See generally Shapiro AI Testimony.