

Before the
FEDERAL TRADE COMMISSION
Washington, DC 20530

In the Matter of)	
Competition and Consumer Protection in the)	Project Number P181201
21st Century Hearings)	Docket Nos. FTC-2018-0049,
)	FTC-2018-0051, FTC-2018-0055,
)	FTC-2018-0056

**COMMENT 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

August 20, 2018

TABLE OF CONTENTS

I.	INTRODUCTION AND SUMMARY	1
II.	INDUSTRY-DEVELOPED, CONSENSUS-BASED GLOBAL STANDARDS BEST ENSURE A COMPETITIVE AND INNOVATIVE MARKETPLACE.....	3
III.	THE FTC SHOULD CONTINUE TO PROMOTE A FLEXIBLE AND TECHNOLOGY-NEUTRAL FRAMEWORK FOR PRIVACY AND SECURITY.....	5
IV.	THE FTC SHOULD CONTINUE TO LOOK TOWARD SELF-REGULATION TO MAINTAIN THE BENEFITS OF EMERGING TECHNOLOGIES AND ADDRESS THEIR CHALLENGES	9
V.	PATENT ASSERTION ENTITIES HINDER INNOVATION	11
VI.	CONCLUSION.....	13

Before the
FEDERAL TRADE COMMISSION
Washington, DC 20530

In the Matter of)	
Competition and Consumer Protection in the)	Project Number P181201
21st Century Hearings)	Docket Nos. FTC-2018-0049,
)	FTC-2018-0051, FTC-2018-0055,
)	FTC-2018-0056

**COMMENT OF THE
CONSUMER TECHNOLOGY ASSOCIATION**

The Consumer Technology Association (“CTA”)¹ is pleased to respond to the Federal Trade Commission’s (“Commission” or “FTC”) Request for Comments (“RFC”) in connection with its public hearings examining “whether broad-based changes in the economy, evolving business practices, new technologies, or international developments might require adjustments to competition and consumer protection law, enforcement priorities, and policy.”²

I. INTRODUCTION AND SUMMARY

Representing an industry responsible for supporting more than 15 million U.S. jobs and generating more than \$377 billion in revenue in the U.S., CTA supports the FTC’s continuing efforts to promote growth and innovation for the internet and the internet-enabled economy. The FTC’s hearings are both welcome and commendable for the reasons that Chairman Simons

¹ The Consumer Technology Association (“CTA”)™ is the trade association representing the \$377 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. Consistent with the instructions in the RFC, CTA notes that it sponsored research cited in footnote 24 of this comment.

² Hearings on Competition and Consumer Protection in the 21st Century, 83 Fed. Reg. 38,307 (Aug. 6, 2018) (“RFC”).

identified: “When the FTC periodically engages in serious reflection and evaluation, [it is] better able to promote competition and innovation, protect consumers, and shape the law, so that free markets continue to thrive.”³ CTA agrees and believes that this proactive effort can help to ensure that the FTC’s priorities remain in step with the marketplace, particularly the ever-changing digital landscape.

Indeed, every government-imposed constraint on technology, whether express regulation or legal standards that develop through enforcement actions, should be balanced against the benefits of innovation. Innovation drives competition and maximizes consumer benefits. Innovation therefore should be a paramount focus and in these hearings and a continued lodestar for the FTC’s activities more generally.

CTA 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[®] 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. Indeed, Eureka Park, the home at the show for startups from around the world, each year exemplifies the tremendous innovation occurring in the technology marketplace.

This comment focuses on two discrete issues raised in the RFC. Sections II-IV discuss “the welfare effects of regulatory intervention to promote standardization and interoperability”

³ See Press Release, Fed. Trade Comm’n, *FTC Announces Hearings On Competition and Consumer Protection in the 21st Century* (June 20, 2018), <https://www.ftc.gov/news-events/press-releases/2018/06/-ftc-announces-hearings-competition-consumer-protection-21st> (Statement of Chairman Simons).

(topic 2).⁴ In this regard, CTA is a strong advocate of voluntary, consensus-based, industry-driven global standards, which best promote innovation by encouraging interoperability and providing a clearer path along which new technologies and services can evolve. By contrast, prescriptive regulations do not afford the same flexibility for industry – whether large, established technology leaders or brand new startups with an idea – to innovate, nor do they allow companies to act quickly and nimbly to address evolving challenges. In addition, Section III and Section IV address issues under topics 4 and 9, respectively: Section III generally addresses privacy and data security regulation, and Section IV addresses regulatory approaches to AI and other emerging technologies.⁵ Section V addresses “the role of intellectual property and competition policy in promoting innovation” (topic 8),⁶ discussing how FTC leadership in the area of so-called patent assertion entities (“PAEs” or “patent trolls”) has been helpful to innovative companies across multiple industries.

II. INDUSTRY-DEVELOPED, CONSENSUS-BASED GLOBAL STANDARDS BEST ENSURE A COMPETITIVE AND INNOVATIVE MARKETPLACE

Voluntary, consensus-based, industry-developed standards are a linchpin in innovation-friendly policies that help to unleash economic development and direct consumer benefits around the world. Industry-developed global standards allow all companies – including small startups and multinational technology leaders – access to the marketplace where they can innovate and compete on the quality and price of their products. Moreover, self-regulatory and other industry-driven, consensus-based approaches not only are nimble enough to address issues posed by

⁴ RFC, 83 Fed. Reg. at 38,308.

⁵ *See id.* at 38,309, 38,310 (soliciting comment on “the intersection between privacy, big data, and competition,” and on the “consumer welfare implications associated with the use of algorithmic decision tools, artificial intelligence, and predictive analytics.”).

⁶ *Id.* at 38,309.

rapidly evolving technologies but also lead to globally harmonized requirements. In turn, they accelerate adoption, drive competition, and enable the cost-effective introduction of new technologies.

The FTC and other federal agencies have recognized the importance of industry-led standards, and CTA has consistently championed their benefits.⁷ As a standards body, CTA is a leader of ongoing efforts to grow the consumer technology industry by developing essential industry standards to enable interoperability between new products on the market and existing devices. CTA's standards committees, which are accredited by the American National Standards Institute, have produced many documents related to the Internet of Things ("IoT") and other emerging technologies. Some of the most recent include, for example: Definitions and Characteristics of Augmented and Virtual Reality Technologies (CTA-2069), Physical Activity Monitoring for Fitness Wearables: Step Counting (ANSI/CTA-2056), and Small Unmanned Aerial Systems Serial Numbers (ANSI/CTA-2063). In addition to its own standards work, CTA helps alliances of companies and professionals within the consumer technology industry like the Open Connectivity Foundation, the Institute of Electrical and Electronics Engineers, and the Internet Engineering Task Force succeed in their efforts to develop and promote security and interoperability standards for the IoT.

Accordingly, the FTC should continue to encourage industry to collaborate in global standardization efforts to develop technological best practices and standards, and also promote regulatory harmonization to increase economics of scales. Moreover, as the Commission

⁷ See, e.g., Comments of the Consumer Technology Association, Docket No. 170105023-7023-01, at 13-14 (filed Mar. 13, 2017), https://www.ntia.doc.gov/files/ntia/publications/cta_comments_on_commerce_-_iot_green_paper-031317.pdf; Comments of the Consumer Technology Association, Docket No. 1603311306-6306-01, RIN 0660-XC024, at 8-9 (filed June 2, 2016), https://www.ntia.doc.gov/files/ntia/-publications/cta_comments_re_ntia_ietf-final-060216_2.pdf. Copies of the CTA filings cited herein are attached.

considers its role in standard setting going forward, in addition to favoring industry consensus-based standards, it should continue to strive for a system where licensing negotiations involving standard essential patents balance the interests of both innovators and implementers while maintaining the main objective of avoiding harm to American consumers. In this regard, the Commission has previously acknowledged its “longstanding commitment” in “preserving the integrity of the standard-setting process” because that “is central to ensuring standard setting works to the benefit of, rather than against, consumers.”⁸

III. THE FTC SHOULD CONTINUE TO PROMOTE A FLEXIBLE AND TECHNOLOGY-NEUTRAL FRAMEWORK FOR PRIVACY AND SECURITY

As CTA has emphasized in various federal regulatory fora, consistent privacy and security protections – two of the foundations of consumer trust – are essential to continuing data-driven innovation and realizing its benefits.⁹ These benefits flow to consumers and businesses alike and generate tremendous economic gains.

In the past, the FTC has recognized that industry self-regulation can protect and inform consumers, while also benefitting honest businesses by addressing deceptive and unfair practices otherwise existing in the marketplace.¹⁰ In addition, self-regulation acts as a force multiplier in terms of extending protections across companies and to consumers, thereby easing the burdens on law enforcement agencies: As the Commission has recognized, “[i]f industry is effective in

⁸ Statement of the Fed. Trade Comm’n, *In the Matter of Robert Bosch GmbH*, FTC File Number 121-0081 (Nov. 26, 2012), <https://www.ftc.gov/sites/default/files/documents/cases/2012/11/121126bosch-commissionstatement.pdf>.

⁹ *See, e.g.*, Comments of the Consumer Technology Association, Docket No. 180124068-8068-01, at 6 (filed July 17, 2018), https://www.ntia.doc.gov/files/ntia/publications/cta_comments_on_ntia_-_international_internet_priorities-final-071718.pdf.

¹⁰ *See, e.g.*, Fed. Trade Comm’n, *Broadband Connectivity and Competition Policy*, at 136 (June 2007), <https://www.ftc.gov/sites/default/files/documents/reports/broadband-connectivity-competition-policy/v070000report.pdf>.

promoting general levels of consumer protection, government agencies can focus their resources on fraud and deception.”¹¹

Indeed, private sector leadership is an effective way to quickly address new privacy and security issues,¹² and CTA and its members are at the forefront of doing so with respect to emerging IoT 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 technology companies.¹³ The Guiding Principles offer an example of how industry can address issues raised by new technologies and services far more nimbly than regulations could.

In addition, CTA is actively undertaking efforts to develop and promulgate voluntary standards for IoT device security. In May 2018, CTA announced that it is working with the Council for Securing the Digital Economy to develop an International Anti-Botnet Guide that will advance best practices across the internet ecosystem to address automated, distributed

¹¹ Fed. Trade Comm’n, *Anticipating the 21st Century: Consumer Protection Policy in the New High-Tech, Global Marketplace*, at 8 (May 1996), https://www.ftc.gov/system/files/documents/reports/anticipating-21st-century-competition-policy-new-high-tech-global-marketplace/gc_v2.pdf.

¹² See Fed. Trade Comm’n, *Implementing the Children’s Online Privacy Protection Act: A Report to Congress*, at 22-23 (Feb. 2007), http://www.ftc.gov/reports/coppa/07COPPA_Report_to_Congress.pdf (finding that self-regulation “often can respond more quickly and flexibly than traditional statutory regulation to consumer needs, industry needs, and a dynamic marketplace”).

¹³ See Press Release, Consumer Technology Association, *Association Unveils First-of-Its-Kind, Industry Supported Principles on Wellness Data Privacy* (Oct. 26, 2015), <https://www.cta.tech/News/Press-Releases/2015/October/Association-Unveils-First-of-Its-Kind,-Industry-Su.aspx>.

threats that harness unsecured devices for malicious purposes.¹⁴ In addition to this internet ecosystem-wide effort, CTA has convened a group of cybersecurity experts to, among other things, organize and increase the visibility of the large body of available security standards, best practices, secure ecosystems, and third-party security certification programs. These efforts to reach all corners of the IoT and technology ecosystem illustrate the coordinated, cross-industry, and global approach that is necessary to address internet security issues.

That said, the emerging fragmentation and inconsistent domestic and international regulatory approaches to privacy and security pose new challenges for companies and threaten to confuse consumers. New legislation and regulation at the state-level already is threatening data-driven innovation. In particular, the California Consumer Privacy Act¹⁵ is a major shift in the privacy landscape – and one that raises some serious concerns for CTA and its members. Moreover, Europe and other regions across the globe increasingly are putting cross-border data flows at risk through new region- or country-specific regulatory obligations and restrictions. While these developments do not warrant a sharp turn from the approach that has served U.S. companies and consumers for well over two decades of massive technological and economic change, they underscore the importance of the FTC’s active involvement in consumer privacy and security going forward. Moreover, it is important that protections are harmonized and flexible, as doing so will benefit consumers and innovation.¹⁶ CTA encourages the FTC to continue to advocate for such an approach, both domestically and abroad.

¹⁴ See Press Release, USTelecom, *CSDE Adds CTA as Strategic Partner on International Anti-Botnet Guide* (May 30, 2018), <https://www.ustelecom.org/news/press-release/csde-adds-cta-strategic-partner-international-anti-botnet-guide-0>.

¹⁵ California Consumer Privacy Act of 2018, http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180AB375.

¹⁶ See Fed. Trade Comm’n, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, at 10 (Mar. 2012), <https://www.ftc.gov/sites/default/files/documents/>

Beyond harmonization, certain key principles should continue to underlie the FTC’s approach to privacy and data security. Specifically:

- **Promote Flexibility.** The FTC has long been the lead U.S. government watchdog for privacy and data security practices, and its flexible case-by-case approach under Section 5 has enabled companies to innovate to develop new data-driven products and services.¹⁷
- **Focus on sensitive data.** Consumer choices and data controls should reflect the sensitivity of personal information. This allows protections to be calibrated to reflect consumers’ expectations and the risks of collecting and using certain types of data, and to avoid pitfalls like over-notifying consumers. It also helps to ensure that the FTC’s approach to privacy focuses in the first instance on practices which could cause concrete, consumer harm. Of course, other considerations, such as the context in which data was collected and is used, and whether such uses are compatible with the purposes for which the data was collected, are also relevant to setting appropriate protections.
- **Maintain technology neutrality.** It is critical to avoid favoring specific technologies or business models. New technologies can raise questions about new concerns and risks, but it is far better for everyone – including businesses and consumers – to recognize this in advance and develop technology-neutral principles from the outset, rather than resorting later to technology-specific regulations, which can stifle innovation and distort the marketplace. The consistent application of these principles through a uniform national framework would further advance the goals of technology neutrality.
- **Promote transparency.** Effective privacy protections begin with businesses providing consumers with clear information about their data practices. Transparency should continue to be a central focus of any privacy framework.
- **Focus enforcement on real harms.** Although an essential component of consumer privacy protections, enforcement should focus on conduct that causes actual harm from alleged privacy or security violations. Enforcement actions that focus on clear legal violations in which consumers suffer harm will help ensure that companies and enforcement agencies use their resources efficiently, in contrast to “gotcha” enforcement.¹⁸

[reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf](https://www.ftc.gov/pressroom/2019/07/120326privacyreport) (“Such interoperability is better for consumers, whose data will be subject to more consistent protection wherever it travels, and more efficient for businesses by reducing the burdens of compliance with differing, and sometimes conflicting, rules.”).

¹⁷ See generally *id.*

¹⁸ As noted above, a focus on sensitive data in particular helps to ensure that the FTC uses its resources to address real and concrete, rather than theoretical, harms to consumers.

Beyond adopting these principles in its own privacy and data security activities, CTA encourages the Commission to advocate these principles in discussions with its counterparts in the states and abroad.

IV. THE FTC SHOULD CONTINUE TO LOOK TOWARD SELF-REGULATION TO MAINTAIN THE BENEFITS OF EMERGING TECHNOLOGIES AND ADDRESS THEIR CHALLENGES

The primary goal of U.S. government policy on emerging technologies should be to promote innovation. Here, again, industry leadership and self-regulation can provide timely responses to consumer protection challenges while preserving the freedom to innovate. As it considers emerging technologies in its policy and enforcement work, the FTC should be guided by the fundamental principle that regulation should narrowly target specific, concrete harms.¹⁹ According to the FTC, “By focusing on practices that have already harmed or are likely to harm consumers,” the agency can address the “most problematic” practices, “while avoiding overly-prescriptive rules that may quickly become obsolete in a rapidly-changing industry.”²⁰ And with respect to nascent technology in particular, the FTC has aptly recognized that premature regulation could stifle innovation.²¹

¹⁹ See Gary Shapiro, *Congress: Want America to Innovate? We need smart regulation*, Medium (Feb. 1, 2017), <https://medium.com/@GaryShapiro/congress-want-america-to-innovate-we-need-smart-regulation-4b760e57c91e> (“By waiting for harm to be demonstrated and practicing a kind of ‘regulatory humility,’ ... new technologies and industries will emerge and thrive.”).

²⁰ Comment of the Staff of the Fed. Trade Comm’n, WC Docket No. 17-108, at 20-21 (filed July, 17, 2017), https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-bureau-consumer-protection-bureau-competition-bureau-economics-federal-trade/ftc_staff_comment_to_fcc_wc_docket_no17-108_7-17-17.pdf.

²¹ See Fed. Trade Comm’n Staff Report, *Internet of Things: Privacy & Security in a Connected World*, at 48-49 (Jan. 2015), <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf> (noting the “great potential” for innovation in IoT, and concluding that IoT-specific legislation would be premature).

Industry's response to the rapid development of AI capabilities illustrates how this works in practice. AI has the potential to transform economies, industries and our everyday lives, improving everything from healthcare to cybersecurity,²² and could contribute over \$15 trillion to the world economy by 2030.²³ 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.²⁴ Again, private sector-led efforts offer the best prospect of identifying and addressing the underlying concerns. For instance, without any government mandate, companies and organizations are developing, sharing, and promoting best practices for the responsible use of AI technologies.²⁵ In addition, CTA itself recently launched an AI working group that includes representatives of companies that are leading in AI development and deployment and understand AI's great potential as well as its risks.²⁶

²² 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>.

²³ See PwC, *Sizing the prize*, <https://www.pwc.com/gx/en/issues/data-and-analytics/publications/artificial-intelligence-study.html> (last visited Aug. 20, 2018).

²⁴ See Consumer Technology Association, *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>.

²⁵ See, e.g., Partnership on AI, <https://www.partnershiponai.org> (last visited Aug. 20, 2018); Google, *Responsible AI Practices*, <https://ai.google/education/responsible-ai-practices> (last visited Aug. 20, 2018); Jerome Pesenti, *AI at F8 2018: Open frameworks and responsible development*, Facebook (May 2, 2018), <https://code.fb.com/ml-applications/ai-at-f8-2018-open-frameworks-and-responsible-development>.

²⁶ Public-private sector collaboration regarding issues like AI's effects on the future of our workforce are far better solutions than the preventative over-regulation of emerging technologies like AI, which will prevent the real benefits and economic potential that such technologies can bring. CTA has sought to address these workforce challenges head-on, including through the creation of CTA's 21st Century Workforce Council. See Testimony of Gary Shapiro, Consumer Technology Association, *Game Changers: Artificial Intelligence Part III, Artificial Intelligence and Public Policy: Hearing Before the H. Comm. on Oversight & Gov't Reform, Subcomm. on Info. Tech.*, 115th Cong. 5 (2018), <https://oversight.house.gov/wp-content/uploads/2018/04/Shapiro-CTA-Statement-AI-III-4-18.pdf>.

The FTC can play helpful role to support these industry efforts. Recognizing AI’s many benefits is one step in that direction. Conversely, substantial consumer benefits from emerging technologies like AI could be lost if discussions focus disproportionately on risk. Consumers generally understand that data powers the smart technologies they use. They recognize that the sweeping benefits of the connected world are not possible without the collection of information and the sharing of information among devices. The FTC should take consumer understanding, as well as ongoing industry efforts concerning AI-related challenges, into account as it examines the impact of AI on consumers and competition.²⁷ CTA urges the FTC to maintain the thoughtful approach it has used with other technologies, and not to simply assume that consumers do not understand these technologies and thus require government intervention to “protect” them.

V. PATENT ASSERTION ENTITIES HINDER INNOVATION

CTA applauds the FTC for shedding light on the harm caused by patent trolls.²⁸ As CTA has emphasized in comments with the FTC, frivolous litigation brought by PAEs not only diverts critical resources away from new product development but also works to reduce the incentives for individuals to create new products, thereby harming competition, innovation, and our

²⁷ RFC, 83 Fed. Reg. at 38,310.

²⁸ See, e.g., Fed. Trade Comm’n, *Patent Assertion Entity Activity: An FTC Study* (Oct. 2016) (“FTC PAE Study”), https://www.ftc.gov/system/files/documents/reports/patent-assertion-entity-activity-ftc-study/p131203_patent_assertion_entity_activity_an_ftc_study_0.pdf.

economy as a whole.²⁹ Approximately \$1.5 billion is drained from the U.S. economy every week that this abuse of the patent system continues.³⁰

The FTC's efforts have brought much-needed attention and analysis to this vital subject. As the FTC examines the "role of intellectual property and competition policy in promoting innovation" (topic 8),³¹ it should continue to call for critical patent reforms that will protect legitimate U.S. business from continued extortion.³² For instance, CTA has supported legislation that would impose heightened pleading standards, place reasonable parameters on discovery, and provide for fee shifting to level the playing field between plaintiffs and defendants in patent suits.³³ At the same time, it is important to stop efforts to undo progress against patent trolls. Any legislation that would roll back gains made against patent trolls in the courts and in the America Invents Act, such as overturning *eBay Inc. v. MercExchange, L.L.C.*,³⁴ or eliminating post-grant patent reviews and the Patent Trial and Appeal Board, would be detrimental to the goal of having intellectual property protections that promote innovation and competition. To this end, the FTC should consider opposing any such measures as they would have deleterious effects on the marketplace.

²⁹ See Comments of the Consumer Electronics Association, Project No. P13203 (filed Dec. 16, 2013), https://www.ftc.gov/sites/default/files/documents/public_comments/2013/12/00066-87874.pdf; Comments of the Consumer Electronics Association (filed April 5, 2013), <https://www.justice.gov/sites/default/files/atr/legacy/2013/04/15/paew-0039.pdf>.

³⁰ See Consumer Technology Association, *Patent Reform*, <https://www.cta.tech/Policy/Issues/Patent-Reform.aspx> (last visited Aug. 20, 2018).

³¹ RFC, 83 Fed. Reg. at 38,309.

³² See FTC PAE Study at 8-13 (supporting many of the reforms for which CTA has advocated, including heightened pleading requirements and changes to address the discovery burden in PAE litigation).

³³ See Press Release, Consumer Technology Association, *CTA Calls for Aggressive Reforms to Crack Down on Patent Trolls, Expresses Support for Inter Partes Reviews and USPTO* (July 12, 2017), <https://www.cta.tech/News/Press-Releases/2017/July/CTA-Calls-for-Aggressive-Reforms-to-Crack-Down-on.aspx>.

³⁴ 547 U.S. 388 (2006).

VI. CONCLUSION

CTA appreciates the FTC's past and current efforts to promote a global, open internet that supports U.S. jobs and economic growth. Although the 21st century digital policy issues that companies face 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 the FTC to continue to keep this principle at the forefront as it moves forward with its competition and consumer protection hearings.

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

August 20, 2018

ATTACHMENTS

Before the
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
Washington, DC 20230

In the Matter of)
)
The Benefits, Challenges, and Potential Roles for the) Docket No. 170105023-7023-01
Government in Fostering the Advancement of the)
Internet of Things)
)
)

**COMMENTS OF THE
CONSUMER TECHNOLOGY ASSOCIATION**

**CONSUMER TECHNOLOGY
ASSOCIATION**

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

March 13, 2017

Table of Contents

I. INTRODUCTION 1

II. RESPONSES TO RFC QUESTIONS 4

A. Is the discussion of IoT in the Green Paper regarding the challenges, benefits, and potential role of government accurate and/or complete, and are there issues that were missed or should be reconsidered? 4

B. Is the approach for Departmental action to advance the IoT comprehensive in areas of engagement, and where does the approach need improvement? 6

C. Are there specific tasks that the Department should engage in that are not covered by the approach? 14

D. What should the next steps be for the Department to foster advancement of IoT? 15

III. CONCLUSION..... 17

Before the
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
Washington, DC 20230

In the Matter of)
)
The Benefits, Challenges, and Potential Roles for the) Docket No. 170105023-7023-01
Government in Fostering the Advancement of the)
Internet of Things)

**COMMENTS OF THE
CONSUMER TECHNOLOGY ASSOCIATION**

I. INTRODUCTION

The Consumer Technology Association (“CTA”)¹ stands for innovators, including the numerous companies – from large household names to entrepreneurial startups – whose products and services largely comprise the Internet of Things (“IoT”). Representing an industry responsible for supporting more than 15 million U.S. jobs and generating more than \$290 billion in revenue in the U.S., CTA looks forward to continuing to work with the Department of Commerce (“Department”) and the new Administration on efforts to promote and further expand the IoT as an engine for U.S. job creation and technological and economic leadership. CTA is pleased to provide comments on the Department’s January 12, 2017 “Green Paper” on fostering the advancement of the Internet of Things.² As CTA’s comments explain, the Green Paper sets

¹ The Consumer Technology Association (CTA)TM is the trade association representing the \$292 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 Department of Commerce, Fostering the Advancement of the Internet of Things (Jan. 2017) (“Green Paper”), https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf. CTA provides its comments in response to the Request for Comment that the National Telecommunications and Information Administration (“NTIA”) issued in connection with the Green Paper. The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of

forth several key ideas that, if implemented, would encourage the rapid and broad adoption of IoT technologies by American businesses, government, and citizens.³

Advances in the IoT, combined with innovation-friendly policies, can help the U.S. unleash economic growth and maintain its global leadership role in technology, including the burgeoning IoT market.⁴ To maintain this position, however, the United States needs to change its recent course of burdensome regulation. Since 2009, federal regulators have issued more than 20,000 rules,⁵ increasing regulatory compliance costs by over \$100 billion annually.⁶ Small businesses, including tech startups, shoulder a disproportionate share of the burden. As CTA consistently has said, government must allow consumers and the market to decide IoT winners and losers, rather than dictate a specific technology solution. This is particularly critical in a nascent market like the IoT, where products and services are in early stages, insight into consumer preferences are just beginning to take shape, and business models are still in flux. Overly broad and prescriptive rules, even when well intended, can inadvertently throttle innovation, prevent beneficial new products from coming to market, and inhibit security innovations that would promote safety. When agencies attempt to proactively resolve problems

Things, 82 Fed. Reg. 4313 (Jan. 13, 2017), <https://www.gpo.gov/fdsys/pkg/FR-2017-01-13/pdf/2017-00720.pdf>.

³ As Commerce Secretary Wilbur Ross stated in his confirmation hearing, all parties with an interest in the Internet of Things “need encouragement.” Commerce Secretary Confirmation Hearing, C-SPAN (Jan. 18, 2017), <https://www.c-span.org/video/?421257-1/commerce-secretary-nominee-wilbur-ross-testifies-confirmation-hearing>.

⁴ See Comments of CTA, Docket No. 1603311306-6306-01 (RIN 0660-XC024), at 2 (June 2, 2016) (“CTA Initial Comments”), https://www.ntia.doc.gov/files/ntia/publications/cta_comments_re_ntia-iot_rfc-final-060216_2.pdf.

⁵ See Maeve P. Carey, Congressional Research Service, *Counting Regulations: An Overview of Rulemaking, Types of Federal Regulations, and Pages in the Federal Register*, at 5-6 (Oct. 4, 2016), <https://fas.org/sgp/crs/misc/R43056.pdf> (listing number of final rules issued by year).

⁶ See James Gattuso & Diane Katz, Heritage Foundation, *Red Tape Rising 2016: Obama Regs Top \$100 Billion Annually* (May 23, 2016), <http://www.heritage.org/government-regulation/report/red-tape-rising-2016-obama-regs-top-100-billion-annually>.

by regulating hypothetical harms, they inevitably choke innovation and unintentionally favor incumbent players with old technologies and standards. Instead, the government should only consider regulating in response to concrete and substantial harms, and then only with technology-neutral policies that do not put disruptive technologies at a disadvantage.⁷

At this stage, bipartisan working groups in the House and Senate, as well as the IoT Caucus, have recognized that the key policy task is to ensure federal policy spurs the innovation economy, while also promoting security and protecting consumers. The Green Paper identifies appropriate priorities along these dimensions, including enabling access to additional flexible-use spectrum; promoting global industry-led standards development (*e.g.*, to support global IoT interoperability); and encouraging the growth and development of open and competitive markets. The Green Paper also suggests a role for the Department in crafting balanced policy and building coalitions on issues such as cybersecurity, privacy, and intellectual property. CTA applauds the Department for identifying these key areas for collaboration and urges the Department to focus on coalition building, public-private partnerships, and industry self-regulation, rather than recommending prescriptive rules. The Green Paper principles generally favor such a targeted, hands-off approach, including reliance on industry-driven, consensus-based, voluntary standards; reducing barriers to entry; and convening stakeholders to address public policy challenges. This is also the best way to encourage privacy and security standards that apply consistently across the digital economy – for the IoT and other connected technologies. By addressing new technologies with this smart and light-touch regulatory approach, the government will empower business leaders to invest time and resources into growing their companies, creating high paying

⁷ Gary Shapiro, *Congress: Want America to Innovate? We Need Smart Regulation*, medium.com (Feb. 1, 2017) (“Shapiro, *Want America to Innovate?*”), <https://medium.com/@GaryShapiro/congress-want-america-to-innovate-we-need-smart-regulation-4b760e57c91e#.ifh8x123b>.

new U.S. jobs, and developing new products and services that will change Americans' lives for the better.⁸

II. RESPONSES TO RFC QUESTIONS

A. **Is the discussion of IoT in the Green Paper regarding the challenges, benefits, and potential role of government accurate and/or complete, and are there issues that were missed or should be reconsidered?**

The Green Paper clearly demonstrates that the Department recognizes the infinite possibilities of the IoT to improve the operations of U.S. companies, enhance the public services provided by all levels of government, and augment and reshape the lives of American citizens.⁹ It discusses the many gains in efficiency, productivity, quality, and safety that the IoT will bring to a broad range of industries, including manufacturing, healthcare, transportation, energy, and retail, and finds that consumers will see benefits through smart homes, vehicle automation, and other connected devices. The Green Paper also notes that the IoT may enable governments to deliver better, cheaper, and more efficient public services, including safety and security services. CTA appreciates the Department's statement that IoT technologies "promise a wide array of safety and efficiency benefits for consumers and businesses alike"¹⁰ and encourages the Department to continue to stay abreast of new IoT technologies and business models as they rapidly evolve. CTA would be pleased to assist in this regard at the Department's request.

The Green Paper concludes that the challenges and opportunities presented by the IoT require a reaffirmation, not a reevaluation, of the well-established U.S. government policy approach to emerging technologies (*e.g.*, encouraging private sector leadership and global

⁸ *See id.*

⁹ Green Paper at 8-10.

¹⁰ *Id.* at 8.

standards development, and using a collaborative multistakeholder approach to policy making).¹¹ This is the right conclusion. As CTA has explained, one of the most significant challenges to U.S. IoT leadership is the existing fragmented approach of federal government agencies toward its development, resulting in inconsistent and reactive policy and regulatory regimes.¹² Toward this end, CTA supports the DIGIT Act, which would give the Department the lead responsibility in identifying regulatory and other barriers to IoT development.¹³ Thus, as the Green Paper finds, coordination among U.S. government partners would be helpful due to the complex, interdisciplinary, cross-sector nature of IoT and may also be useful when working with international and private sector partners.¹⁴ The Green Paper correctly concludes that the government will need to maintain its robust advocacy for industry-led approaches and consensus-based standards on the global stage and should continue to use multistakeholder approaches.¹⁵ To do so, as the Green Paper notes, the Department can look to its successful efforts to date in building flexible and adaptable frameworks, codes of conduct, and best practices.¹⁶ CTA further encourages government to invest in these multistakeholder efforts, as the IoT continues to evolve.

¹¹ The Green Paper correctly focuses on scope (IoT connects a wider range of systems and devices than ever before), scale (the magnitude of connected devices), and stakes (“A major internet outage or a cyberattack would never have been without consequence, but IoT raises the stakes significantly, as such events can now affect medical devices, supply chain reliability, and cars driving down the highway, raising the real possibility of physical harm.”). *Id.* at 4 (citation omitted).

¹² *See* CTA Initial Comments at 4.

¹³ For further discussion of the DIGIT Act, see *infra* section II.D.

¹⁴ Green Paper at 10-13. CTA encourages the Department to continue including digital economy issues in its formal government-to-government dialogues with top trading partners and to support continued IoT engagement internationally.

¹⁵ *Id.* at 11.

¹⁶ *Id.* at 12-13.

B. Is the approach for Departmental action to advance the IoT comprehensive in areas of engagement, and where does the approach need improvement?

Consistent with CTA's initial comments, the Green Paper sets forth Departmental priorities that include enabling access to flexible-use spectrum, promoting global standards and technology advancement, and encouraging markets (for example, through public-private partnerships and workforce education and training).¹⁷ CTA applauds the Department for recognizing the "significant role" wireless technologies will play in supporting connected devices, with IoT apps "leverag[ing] . . . 5G [] technologies, innovative unlicensed use of spectrum, and low-power connectivity protocols, among other advances," and for understanding that a "shortage of available spectrum could become a constraint on the growth of IoT."¹⁸

Indeed, to connect the tens of billions of devices expected to be in use by 2020, some estimates suggest that networks would require capacity that is "at least 1,000 times the capability that exists today."¹⁹ With the IoT showing promise in so many sectors of the U.S. economy, a broad range of agencies must coordinate amongst themselves and partner with industry to ensure sufficient spectrum for the IoT. The wide variety of IoT spectrum uses means that NTIA must help facilitate sharing or clearing of federally controlled spectrum. Given the cross-cutting nature of IoT, agencies must collaborate to enable the IoT to flourish. As Commerce Secretary Wilbur Ross said at his confirmation hearing, "[w]e need more spectrum in the private sector, and I will try my best to help convince those government agencies that have spectrum and don't

¹⁷ See CTA Initial Comments at 15-16.

¹⁸ Green Paper at 16-18.

¹⁹ See CTA Initial Comments at 9 (citing Murray Slovick, *5G: The Mobile Tech of 2020*, CONSUMER ELECTRONICS ASSOCIATION I³, 20, 22 (Nov./Dec. 2014), <http://cdn.coverstand.com/25838/232265/-711ba5485b2b1c66036f89c895b2baecbaa98e91.23.pdf>).

really need it to permit it to be commercialized.”²⁰ He appropriately concluded that while we cannot compromise national defense, we must be rational and combat spectrum hoarding. This is especially true where exclusive spectrum was allocated over a decade or more ago and it is possible that today’s technology advancements can enable efficient spectrum sharing.

Although opening additional licensed and unlicensed spectrum for new innovation, including innovation based on new, globally harmonized technologies like 5G, will be foundational to promoting the growth of the IoT, there is a broader and more significant infrastructure objective if America is to lead the world for decades to come: Government must incentivize cutting-edge IoT solutions to advance the Administration’s broader infrastructure rebuilding and development goals – by incorporating smart technologies into public infrastructure projects. The Department correctly observed that “infrastructure investment, innovation, and resiliency (such as across the information technology, communications, and energy sectors) will provide a foundation for the rapid growth of IoT services.”²¹ CTA encourages the Department to pursue the next steps proposed in the Green Paper, including coordinating with private sector, federal, state, and local government partners to ensure infrastructure continues to expand and remains innovative, open, secure, interoperable, and scalable.²² CTA looks forward to engaging with the Department on these efforts to leverage “smart,” forward-looking solutions in the nation’s transportation, energy, and security

²⁰ Amir Nasr, *Here’s What Ross Said About Tech Policy During His Confirmation Hearing*, Morning Consult (Jan. 18, 2017), <https://morningconsult.com/2017/01/18/heres-ross-said-tech-policy-confirmation-hearing> (Testimony of Wilbur Ross).

²¹ The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things, 81 Fed. Reg. 19956, 19959 (Apr. 6, 2016) (“RFC”), <https://www.gpo.gov/fdsys/pkg/-FR-2016-04-06/pdf/2016-07892.pdf>.

²² Green Paper at 23-24.

infrastructure, as well as opportunities to invest in infrastructure that will accelerate U.S. leadership in innovative technologies like autonomous vehicles.

The Green Paper also finds that the Department should craft balanced policy and build coalitions on issues including cybersecurity, privacy, intellectual property, and cross-border data flows. While government has a critical role to play in ensuring that its policies enable industry to meet consumers' IoT demands, it must be sure to limit other types of regulatory intervention – and to refrain from issuing any regulations that could stifle innovation in the nascent IoT ecosystem. Prescriptive regulation, however well intentioned, could inhibit the development and deployment of such offerings. The Department, and the Administration as a whole, should ensure that government assesses any potential need for IoT regulation in a coordinated manner and, if it identifies a need for regulation is necessary, avoids creating fragmented or conflicting requirements. Policymakers at all levels of government should exercise restraint, given the complexity of the IoT and the vast potential for unintended consequences, and take only actions consistent with the core framework discussed in CTA's initial comments:²³

- The primary goal of any IoT policy regime should be to promote innovation.
- To promote innovation, policymakers should favor market-based solutions over prescriptive regulations and apply regulation only if there is a compelling public interest in doing so (*i.e.*, in order to address demonstrable harms that cause concrete injury to consumers).²⁴ Such an approach is consistent with President Trump's executive actions instituting a regulatory freeze and requiring federal agencies to

²³ See CTA Initial Comments at 16-19.

²⁴ See Shapiro, *Want America to Innovate?*; Gary Shapiro, *HowThe Heavy Hand Of Government Stifles The On Demand Economy*, TECHDIRT (Aug. 25, 2015), <https://www.techdirt.com/articles/20150824/-11370432049/how-heavy-hand-government-stifles-demand-economy.shtml>.

minimize the net costs to the private sector of any new regulations.²⁵ CTA encourages the Department, as well as all federal agencies and the Administration, to review any new or proposed regulations with this in mind.

- If policymakers decide that some form of oversight is appropriate in a given case, they should proceed with caution, favoring self-regulation over command-and-control outcomes.

Consistent with these principles, policymakers should avoid imposing mandates that would pick technology winners or otherwise impede the growth of the IoT, such as by precluding market competition. Government also must refrain from over-reaching enforcement actions that harm consumers by increasing the cost of providing service and entering a sector without providing commensurate consumer benefit.

Cybersecurity and Privacy. The security and privacy issues associated with the IoT closely mirror those in which industry already has a strong track record of developing and implementing best practices to protect consumers. A lesson learned from experience with the internet economy over the past couple of decades is that consistent, effective privacy and security protections – a foundation of trust – are most likely to develop when the government itself takes a holistic view of technologies, business models, and privacy and security risks. The IoT is no different. Thus, to address privacy and security concerns, government should continue to foster global, industry-wide, consensus-driven self-regulation that is nimble and accounts for rapidly evolving technologies.²⁶ In the Green Paper, the Department proposes to support and

²⁵ See Exec. Order No. 13771, Reducing Regulation and Controlling Regulatory Costs, 82 Fed. Reg. 9339 (Feb. 3, 2017), <https://www.gpo.gov/fdsys/pkg/FR-2017-02-03/pdf/2017-02451.pdf>; Memorandum for the Heads of Executive Departments and Agencies; Regulatory Freeze Pending Review, 82 Fed. Reg. 8346 (Jan. 24, 2017), <https://www.gpo.gov/fdsys/pkg/FR-2017-01-24/pdf/2017-01766.pdf>.

²⁶ See CTA Initial Comments at 19.

promote policies that encourage risk-based approaches, security by design, and the ability to patch insecure software and devices; promote the use of strong encryption; and collaborate with industry on security and safety education for consumers.²⁷ CTA concurs.

The Green Paper recognizes that while the IoT presents some security risks to connected vehicles and consumer devices, for example, the range of IoT devices and apps precludes a single, prescriptive solution. The Department concluded that the U.S. government can play a valuable role in driving awareness and resolution of the cybersecurity issues facing IoT development. Multistakeholder efforts and industry-driven global standards organizations are very important in this regard and have a track record of success. For example, the NIST Cybersecurity Framework – developed through the public-private partnership work of multiple critical infrastructure sectors with the Department – “highlights the limitations of a ‘one-size-fits-all’ solution and instead is a voluntary, flexible framework that can be scaled to organizations’ different needs, allowing them to take into account particular business models, assets, and other variables.”²⁸ 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.²⁹ A similar approach could address consumer safety and quality of

²⁷ Green Paper at 42-43.

²⁸ *Id.* at 27; *see also* CTA Initial Comments at 25; U.S. Communications Sector Coordinating Council, <https://www.comms-scc.org/about-1> (last visited Mar. 10, 2017) (describing means of coordination used by the Communications Sector Coordinating Council); FCC, Advisory Committees, *Communications Security, Reliability and Interoperability Council*, <http://transition.fcc.gov/pshs/-advisory/csric> (last visited Mar. 10, 2017). The Communications Security, Reliability and Interoperability Council’s (“CSRIC”) working groups have proposed implementation guidance to help communications companies implement the NIST Cybersecurity Framework and continue to recommend and refine best practices in this space. CSRIC, *Cybersecurity Risk Management and Best Practices, Working Group 4: Final Report* (Mar. 2015), https://transition.fcc.gov/pshs/advisory/-csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.

²⁹ *See, e.g.*, Stakeholder Engagement on Cybersecurity in the Digital Ecosystem, 80 Fed. Reg. 14360, 14360 (Mar. 19, 2015), <https://www.gpo.gov/fdsys/pkg/FR-2015-03-19/pdf/2015-06344.pdf> (recognizing that traditional regulation in this context is “difficult and inefficient” in light of the “pace of innovation in the highly dynamic digital ecosystem”); *id.* at 14361 (stating that “[i]n the digital ecosystem, the rapid

service issues in the IoT by giving industry the opportunity to directly participate and shape practices that can evolve as new business and technological developments emerge. By significantly expanding the number of potential incursion points for malware, botnets and other forms of cyber threats, the IoT unquestionably presents serious security issues that must be grappled with by all elements of the marketplace, including device makers, product dealers, hardware and software vendors, service providers, and other stakeholders. The Department's experience and track record in convening multistakeholder processes will be critical to helping to forge holistic solutions to IoT security issues.

The Green Paper advocates security by design and notes that the Federal Trade Commission ("FTC") has also embraced this approach with its IoT "Start with Security" guidance.³⁰ CTA concurs that security must be integrated into the hardware and the software at the outset to enable robust, secure, trusted end-to-end IoT solutions. Multi-layered protection must at least protect storage, and enable device identification and authentication, software authentication, protected boot and trusted execution environment. Indeed, security should be integrated throughout the concept and design process. Attempts to bolt on security features late in the product development process are more expensive, more difficult, and prone to error. However, there is no clear consensus or straightforward path on how to implement this concept across the IoT space.

pace of innovation often outstrips the ability of regulators to effectively administer key policy questions," and that "[o]pen, voluntary, and consensus-driven processes can work to safeguard the interests of all stakeholders while still allowing the digital economy to thrive"); Angela Simpson, Deputy Assistant Sec'y of Commerce for Comm'ns and Info., NTIA, Remarks on the Vulnerability Research Disclosure Multistakeholder Process (Sept. 29, 2015) ("[I]t is not our job to tell you what to do. NTIA will not impose its views on you. We will not tip the scales. We are not regulators. We are not developing rules. We do not bring enforcement actions. Instead, we are in a unique position to encourage you to come together, to cooperate, and to reach agreement on important issues"), <http://1.usa.gov/1XvgMFd>.

³⁰ Green Paper at 27.

CTA also recognizes that security plays an important role in protecting consumers' privacy. Similar to other technologies, with regard to broader questions of privacy, CTA urges the Department to maintain the Green Paper's perspective of collaborating with industry experts in multistakeholder efforts and looking to existing policies and frameworks to address these questions. Although IoT devices can collect different types of personal data, or increase the amount of personal data that companies collect, a time-tested technology-neutral privacy framework based on transparency, consumer choice, security, and heightened protections for sensitive data should remain the foundation of privacy protections for the IoT, as for all other technologies. There is no need for a special or different set of privacy rules to apply to IoT devices, and such an approach would stifle – rather than advance – the evolution of the IoT marketplace.

CTA also urges the Department to recognize that a wide range of self-regulatory regimes help companies develop business practices and customer notices that effectuate their privacy obligations and safeguard consumer information privacy while fostering innovation.³¹ Stakeholders already are proactively addressing IoT privacy concerns through such efforts.³² Government action cannot match the speed and agility of these efforts, though the government – particularly the FTC – can play a helpful role in ensuring that companies keep the promises that they make to consumers about privacy protections.

Intellectual Property. The Green Paper concludes that intellectual property deserves further consideration as IoT becomes more ubiquitous.³³ It notes that patents provide incentives

³¹ See CTA Initial Comments at 19.

³² See *id.* at 19-20. Broadband Internet Technical Advisory Group, *Internet of Things (IoT) Security and Privacy Recommendations*, Uniform Agreement Report (Nov. 2016), [https://www.bitag.org/documents-/BITAG_Report_-_Internet_of_Things_\(IoT\)_Security_and_Privacy_Recommendations.pdf](https://www.bitag.org/documents-/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf).

³³ Green Paper at 33-34.

for innovators to develop better IoT devices, manufacturing practices, and infrastructure; there may be issues around standard essential patents and licensing, as well as patent quality.³⁴ The Department’s U.S. Patent and Trademark Office (“USPTO”) can continue its efforts to improve “patent quality, especially in new technological domains, including IoT.”³⁵ As more “things” become embedded with patentable technologies, the “attack surface” for patent assertion entities – better known as “patent trolls” – grows. Patent reform, enabled by Congress and implemented by the USPTO, aimed at blunting patent trolls will remove a harmful tax on IoT development.

Standards development. As CTA noted in its response to NTIA’s initial Request for Comments, voluntary, consensus-based, global standards are best positioned to help advance IoT development and innovation because they promote interoperability and provide a clearer path along which technologies can evolve.³⁶ Proprietary or country-specific standards must be discouraged. CTA applauds the Green Paper’s recognition of the benefits of this role for voluntary, consensus-based global standards, as well as the roles that NIST and NTIA have played in promoting the development of such standards. CTA encourages the Department to continue this work in connection with IoT-related standards, in addition to engaging with its foreign counterparts to promote voluntary standards development. Although no single forum can develop all of the standards for the IoT, maintaining a consistent approach with private sector leadership at its center provides the best chance of success in this broad endeavor. A few examples of leading global standards organizations with broad-based memberships are the Industrial Internet Consortium (“IIC”),³⁷ the Open Connectivity Foundation (“OCF”)³⁸ and the

³⁴ *Id.* at 36.

³⁵ RFC at 19958.

³⁶ CTA Initial Comments at 8-9.

³⁷ *See* Industrial Internet Consortium, <http://www.iiconsortium.org> (last visited Mar. 10, 2017).

OpenFog Consortium (“OpenFog”).³⁹ The IIC’s more than 250 members published a security framework for the Industrial IoT last year, and the organization has 27 active test beds spanning multiple sectors around the globe and 25 more test beds in the pipeline. The OCF includes hundreds of members from diverse market sectors around the world and is developing an interoperability specification, an open source implementation, and a certification program to ensure interoperability regardless of manufacturer, form factor, operating system, service provider or physical transport technology. OpenFog has over 60 members and is growing, and has published a fog computing architecture overview in 2016 (fog computing is a type of IoT architecture), with the reference architecture framework slated for this year. CTA encourages the Department to promote the efforts of the IIC, OCF, OpenFog and other leading industry-driven, global standards organizations with large U.S. participation, such as CTA, to advance IoT innovation and development.

C. Are there specific tasks that the Department should engage in that are not covered by the approach?

The Department can work with other government entities to take additional steps toward ensuring that the U.S. IoT sector maintains its global leadership role. For example, through procurement, the government can generate demand for IoT technologies to help jumpstart the development of IoT ecosystems. In addition, changes in tax policy can help facilitate the rapid growth of the IoT sector, and more attention needs to be given to the unintended consequences of tax policies on the IoT market. Tax laws should foster IoT innovation rather than providing disincentives to the continued rapid deployment of the IoT, which should be driven by competition and consumer demand.

³⁸ See Open Connectivity Foundation, <https://openconnectivity.org> (last visited Mar. 10, 2017).

³⁹ See OpenFog Consortium, <https://www.openfogconsortium.org/about-us> (last visited Mar. 10, 2017).

Another area for government action is immigration, ensuring that appropriate immigration policies are in place to grow the U.S.'s science, technology, engineering, and math ("STEM") work force to unleash the potential of the IoT sector. Strategic immigration reforms are needed to encourage U.S.-educated immigrants to remain in the U.S. to build businesses and create domestic jobs.

Finally, as discussed to some extent in the Green Paper, there is a role for government in consumer education. Building a strong partnership between the public and private sectors can help bolster the foundation for consumer confidence and trust in the IoT. As the Green Paper notes, government can play an active role in skills development to create quality career paths and can incorporate IoT into education and awareness programs.⁴⁰ At a fundamental level, the IoT depends on the collection and sharing of information among devices, and thus is premised on consumer trust and utility. In addition to the work already being done by IoT manufacturers and service providers, government can advance the interests of consumers by working with industry to develop a system of trust between users and things. Together, following the FTC's example in its *Start with Security* series, government and industry can work to educate consumers on issues such as how to limit risks associated with unsecured connected devices (*e.g.*, by changing default passwords, using password-protected home Wi-Fi networks with firewalls, and employing virtual private networks).

D. What should the next steps be for the Department to foster advancement of IoT?

The Green Paper proposes numerous next steps for the Department to take to help advance the IoT. Many of these proposals are consistent with CTA's perspectives on the specific subject matter areas discussed above, from global standards to spectrum to workforce

⁴⁰ Green Paper at 54.

development. These steps would meaningfully advance IoT development. Still, CTA remains concerned about the differing approaches of the many federal agencies that are active in IoT policy formulation. In order to best foster advancement of IoT in the U.S. and ensure that America leads the world, we must have a national IoT strategy that emphasizes the need to handle the IoT with a light regulatory touch and makes a commitment to coordinating federal agencies' IoT policy development activities.

As a further first step, CTA strongly encourages the Department to support the bipartisan “Developing Innovation and Growing the Internet of Things (DIGIT) Act,” which would require the Secretary of Commerce to convene a working group of Federal stakeholders to provide IoT recommendations to Congress, in consultation with industry and non-governmental stakeholders.⁴¹ While the Department’s Green Paper “defer[red] to future policy makers to determine the value of crafting a national strategy[,]”⁴² CTA respectfully suggests that, it is an opportune time for the Department to support the DIGIT Act as a step toward developing collaborative recommendations that can inform a national IoT strategy and, in turn, developing such strategy. A collaborative, pro-innovation IoT strategy will help solve important societal issues and drive American competitiveness for decades to come – fueling GDP, creating new jobs, and bolstering the U.S. economy.

The Department’s range of expertise makes it a logical choice to play a leading role in that effort. The Department also has an overall focus on promoting innovation, economic growth, and job creation – all of which will follow from an IoT policy that avoids new prescriptive regulations and eliminates duplicative or conflicting mandates that currently exist.

⁴¹ Developing Innovation and Growing the Internet of Things Act, S. 88, 115 Cong. (2017) (“DIGIT Act”), <https://www.gpo.gov/fdsys/pkg/BILLS-115s88is/pdf/BILLS-115s88is.pdf>.

⁴² Green Paper at 10.

For these reasons, CTA supports having the Department take a lead role in developing an Administration policy that more comprehensively positions the United States to ensure its IoT leadership and to realize the IoT's full economic and social benefits.

III. CONCLUSION

The Department is uniquely positioned to advance policies that will help develop the IoT and advance the Administration's broader economic goals. By supporting the DIGIT Act and a national IoT strategy; making more flexible-use spectrum available; convening stakeholders to address IoT issues and incentivizing IoT solutions for next generation infrastructure; promoting voluntary, global consensus-based, industry-driven standards; supporting multistakeholder and industry efforts to drive innovation in security innovation; and harmonizing federal agency interaction – the Department has a key role to play in bringing the full benefits of the IoT to U.S. consumers, businesses, and society. In addition, the Department can promote policies that will build – and expand – a workforce that possesses the skills necessary to fully realize the IoT's potential benefits. These actions will drive United States' global leadership in the transformative IoT ecosystem. By contrast, broad, prescriptive regulatory action would derail or delay new IoT applications in the U.S., to the nation's global disadvantage. The Department should use its role in the federal government as well as its activity in international fora to promote voluntary, industry-driven global technical standards and self-regulatory approaches that promote innovation and protect consumers, rather than stifling growth with burdensome and inflexible regulations. The actions suggested in the Green Paper represent a solid step toward achieving these goals, and CTA looks forward to working with the Department and the Administration as it ensures America's IoT competitiveness and leadership into the future.

Respectfully submitted,

CONSUMER TECHNOLOGY
ASSOCIATION

By: /s/ Julie M. Kearney

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

March 13, 2017

Before the
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
Washington, DC 20230

In the Matter of)
)
The Benefits, Challenges, and Potential Roles for the) Docket No. 1603311306-6306-01
Government in Fostering the Advancement of the) RIN 0660-XC024
Internet of Things)
)
)

**COMMENTS OF
THE CONSUMER TECHNOLOGY ASSOCIATION
F/K/A THE CONSUMER ELECTRONICS ASSOCIATION**

**CONSUMER TECHNOLOGY
ASSOCIATION F/K/A CONSUMER
ELECTRONICS ASSOCIATION**

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

June 2, 2016

Table of Contents

I.	INTRODUCTION	1
II.	RESPONSES TO RFC QUESTIONS	4
A.	Challenges and Opportunities Arising from IoT (Question 1)	4
B.	Definition to Use in Examining the IoT Landscape (Question 2); Ways to Divide or Classify the IoT Landscape to Improve the Precision with which Public Policy Issues are Discussed; Benefits or Limitations of Using Such Classifications (Question 4).....	7
C.	Current or Planned Laws, Regulations, and/or Policies that Apply to IoT (Question 3)	8
D.	Technological Issues That May Hinder IoT Development (Question 6).....	8
E.	Factors the Department and Government More Generally Should Consider When Prioritizing Technical Activities with Regard to IoT (Question 7)	11
F.	Role of Government in Bolstering and Protecting Availability and Resiliency of Infrastructures to Support IoT (Question 10).....	12
G.	How Government Should Quantify and Measure the IoT Sector (Question 11); How Government Should Measure the Economic Impact of IoT (Question 12)	14
H.	Impact of the Growth of IoT on the U.S. Workforce and Potential Benefits for Employees and/or Employers (Question 14)	15
I.	How Government Should Address the Main IoT Policy Issues (Question 15)	16
J.	How Government Should Address IoT Cybersecurity and Privacy Concerns (Questions 16-17).....	19
K.	Ways that the IoT Affects and is Affected by Questions of Economic Equity (Question 19)	22
L.	Factors and Issues the Department Should Consider in its International Engagement (Questions 20-23).....	24
M.	IoT Policy Areas that Could be Appropriate for Multistakeholder Engagement; Role the Department of Commerce Should Play in Addressing IoT Challenges and Opportunities and Collaborating with Stakeholders; Government and Private Sector Collaboration to Ensure that Infrastructure, Policy, Technology, and Investment are Working Together to Fuel IoT Growth and Development (Questions 25-27)	25
N.	Additional Relevant Issues (Question 28)	27
III.	CONCLUSION.....	29

Before the
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
Washington, DC 20230

In the Matter of)
)
The Benefits, Challenges, and Potential Roles for the) Docket No. 1603311306-6306-01
Government in Fostering the Advancement of the) RIN 0660-XC024
Internet of Things)

**THE CONSUMER TECHNOLOGY ASSOCIATION
F/K/A THE CONSUMER ELECTRONICS ASSOCIATION**

I. INTRODUCTION

The Consumer Technology Association (“CTA”)¹ applauds the Department of Commerce (“Department”) for its continued effort to promote the Internet of Things (“IoT”), and, in particular, for issuing the above-captioned Request for Comment (“RFC”)² soliciting input on how to develop a more cohesive federal government approach that will foster IoT innovation and economic growth.³ CTA is proud to represent the companies whose products and

¹ The Consumer Technology Association (“CTA”)TM, formerly the Consumer Electronics Association (“CEA”)[®], is the trade association representing the \$285 billion U.S. consumer technology industry. 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 technology. Profits from CES are reinvested into CTA’s industry services.

² *The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things*, Request for Public Comment, Docket No. 1603311306-6306-01, RIN 0660-XC024, 81 Fed. Reg. 19,956 (Apr. 6, 2016) (“RFC”).

³ See Davidson and Kinney, *supra*; see also Lawrence E. Strickling, Assistant Sec’y of Commerce for Comm’n and Info., Dep’t of Commerce, Keynote Address at the Silicon Flatirons Conference on the Digital Broadband Migration: The Evolving Industry Structure of the Digital Broadband Landscape (Jan. 31, 2016) (indicating that the National Telecommunications and Information Administration, an agency within the Commerce Department, would issue a request for comment regarding whether there are policy areas related to the IoT that could be appropriate for multistakeholder engagement), <http://1.usa.gov/1sOUaVa>.

services largely comprise the IoT and looks forward to working with the Department and other stakeholders on this initiative.

The RFC aptly recognizes that the IoT “has quickly become one of the most important technological trends of this decade. It touches almost every industry and will transform our lives and society worldwide.”⁴ Indeed, whether you call it the “Internet of Things,” the “Internet of Everything,” the “Connected World,” or just plain amazing, the rapidly expanding thread of connectivity among everyday objects via the Internet unquestionably is changing how the world works. Thermostats, refrigerators, and even whole factories of equipment can harness the power of the Internet to provide enormous personal, economic, and societal benefits—some we already see, and some are yet to be imagined. Today, consumer- and industrial-facing IoT applications save consumers and businesses time and expense, increase efficiency and productivity, promote public health and safety, and serve as key economic drivers that enhance the U.S. role as a global leader in technology.⁵

Nowhere are the opportunities and promise of the IoT more evident than at the annual CES in Las Vegas, which is the most popular technology trade show in the world and arguably the most important annual innovation event worldwide. From around the globe, thousands of companies display an awe-inspiring vision of the future and showcase the latest and greatest IoT technologies. Walking the show floor in 2016, visitors saw a vision of the connected world that was jaw-dropping in its expanse and potential: multitudes of devices communicating with each other to improve quality of life across many metrics, with enormous potential to beneficially transform our lives and society. Its seamless connectivity, made possible by increased

⁴ Press Release, Dep’t of Commerce, *U.S. Department of Commerce Seeks Comment on Potential Policy Issues Related to Internet of Things*, Apr. 5, 2016, <http://1.usa.gov/1ozo253> (“Comment Press Release”).

⁵ *Id.* (“The explosive growth of connected devices promises both enormous benefits and complex challenges in areas such as health, safety, energy, security, and the environment.”).

processing power and tiny sensors, will enable machines and devices to respond to conditions and situations pursuant to parameters dictated by a consumer—for example, running the washing machine at a time of day when energy costs are low. The IoT connected world will improve energy conservation, efficiency, productivity, public safety, health, education, and more. It will enable more smart homes and appliances, smart cars, smart retail experiences, smart agriculture and manufacturing, and smart devices we cannot imagine today. These connected devices and machines will make our lives easier, safer, healthier, less expensive, and more productive.

This is just the beginning, and there is no telling what the future holds. As Assistant Secretary Strickling explains, “We are just beginning to see the exciting range of novel applications and connected devices emerging from the Internet of Things.”⁶ Explosive gains in IoT connectivity and the lightning-fast speed of innovation in general are driving strong growth across countless tech categories, as well as sparking growth with new capabilities and new business models across multiple industry sectors. As highly sophisticated technology becomes more affordable and accessible, new innovations will help improve our safety, productivity, and entertainment. And the next evolution of the IoT will build on connections already in place. As products become smart and connected, consumers will be able to manage their lives and engage in work in ways that were not even imaginable a decade ago.

The Department’s green paper to be produced based on input responding to the RFC should recognize that policymakers must work *with* industry to ensure that any actions taken in the name of consumer protection do not inadvertently hamstring the myriad consumer-friendly IoT developments. Government must allow consumers and the market to decide IoT winners and losers, rather than dictating outcomes itself. Policymakers thus should focus on private

⁶ *Id.*

sector, consensus-driven industry self-regulation, which has a proven history of minimizing consumer harms while maximizing flexibility to innovate, instead of government action that threatens to curb innovation.

In addition, policymakers should encourage and support growth and adoption of the IoT through efforts to spur research and development, lower effective tax rates, adopting immigration policies that allow U.S. companies to attract the best and brightest, and aggressively facilitating access to spectrum. The government can best promote consumer confidence and trust in the IoT under applicable *existing* statutes and regulations; these existing legislative and regulatory vehicles will ensure protection of consumer privacy, sensitive data, and network security.

II. RESPONSES TO RFC QUESTIONS

A. Challenges and Opportunities Arising from IoT (Question 1)⁷

A significant challenge presented by the IoT is the current fragmented approach of federal government agencies toward its development. The RFC notes that a number of federal agencies—for example, the National Highway Traffic Safety Administration (“NHTSA”) and the Food and Drug Administration (“FDA”)—have already begun grappling with potential health, safety, and security issues arising from the connection of cars and medical devices to the Internet, while the Federal Trade Commission (“FTC”) has identified consumer privacy and cybersecurity aspects of IoT and proposed some possible best practices, and the Administration is sponsoring grants for Smart Cities through no less than five agencies. Many of these efforts are critical to the long-term success of the IoT, but the fragmentation is potentially damaging.⁸

⁷ Section I, above, also discusses the opportunities and benefits of the IoT.

⁸ See Darren Samuelsohn, *What Washington really knows about the Internet of Things*, Politico (“new networked-object technologies are covered by at least two dozen separate federal agencies—from the [FDA] to the National Highway Traffic Safety Administration (“NHTSA”), from aviation to agriculture—and more than 30 different congressional committees”), <http://politi.co/1Kk0usb>.

This fragmentation and duplication of effort reflects the fact that, as the RFC notes, “some types of devices will fall into readily identifiable commercial or public sectors in their own right—for example, implantable health devices—but most will serve the function of enabling existing industries to better track, manage, and automate their core functions.”⁹ The FDA’s rules and the Health Insurance Portability and Accountability Act (“HIPAA,” enforced by the Department of Health and Human Services) may apply to a wearable offered by your health provider, whereas the same device, purchased in a retail store, may be regulated in an entirely different manner, such as by the FTC. Meanwhile, the federal agency that has been the most involved in exploring the consumer IoT, the FTC, is focused on a case-by-case law enforcement approach and providing broader guidance by interfacing with IoT companies by convening workshops and issuing business guidance but ultimately its legal authority has some limitations.¹⁰ Thus, the specific laws, rules, and regulatory regime(s) that apply to a particular IoT device or application may not always be obvious and may even overlap or conflict, and this complex web may be particularly difficult for smaller companies unable to afford counsel for each regime to navigate.

These challenges are exacerbated as innovation eviscerates historical distinctions between different types of services and applications. As the Department’s Alan Davidson and Linda Kinney recently described,

Regulators have long been focused on health and safety regulations that protect consumers; but in the past, enterprises in the transportation,

⁹ RFC at 19,957.

¹⁰ On the other hand, the FTC’s general Section 5 authority covers broad swaths of industries, and thus it is not constrained on a sector-specific basis in the same way as is, for example, the Federal Communications Commission (“FCC”). The FTC can set parameters through enforcement actions based on specific entities’ business practices that are deceptive or unfair to consumers (*e.g.*, failing to adequately protect consumer data or not meeting the terms of a privacy policy or other representations to the consumer).

healthcare, and communications sectors have mostly functioned and been regulated independently. Now our physical and digital worlds are converging and lines between industries are increasingly blurred. Automobiles are becoming communications devices on wheels.... [T]he Internet of Things is breaking down traditional silos....¹¹

Moreover, legislative and regulatory vehicles that would focus on IoT-specific technologies, rather than IoT as part of larger and more comprehensive legislation, or inappropriate use of a given IoT application, are a mistake. They would threaten to put the government in the position of picking winners and losers to the detriment of competition, innovation, economic growth, and, ultimately, consumer and societal welfare. Instead, policymakers should focus on desired outcomes and results, and let the pace of innovation and market dynamics determine which IoT technologies prevail. The Department's own staffing structure recognizes this challenge, which it describes as "the cross-cutting nature of the IoT landscape."¹²

Of course, there are other challenges to the success of the IoT beyond inconsistent, premature, and reactionary regulatory regimes. At a fundamental level, the IoT depends in great part on the collection and sharing of information among devices and machines, and thus is premised on consumer trust, data accuracy, and utility. IoT manufacturers and service providers take seriously the need for consumer trust and, both as individual companies and as industries, have proactively addressed these issues. Moreover, the current lack of IoT technical standards muddies the water for players in the IoT ecosystem, who have no agreed-upon regimen for how

¹¹ Alan Davidson and Linda Kinney, *Fostering Investment and Innovation in Smart Cities and the Internet of Things (IoT)*, NTIA (Feb. 25, 2016, 3:52 PM) (this "growing global patch of regulation threatens to increase costs and delay the launch of new products and services", which "in turn, could dampen investment"), <http://1.usa.gov/1Q5i5Xd>.

¹² RFC at 19,958.

to connect or interoperate. As discussed below, the Department can take several steps to encourage and support the IoT.

B. Definition to Use in Examining the IoT Landscape (Question 2); Ways to Divide or Classify the IoT Landscape to Improve the Precision with which Public Policy Issues are Discussed; Benefits or Limitations of Using Such Classifications (Question 4)

CTA recommends that the Department consider consumer-facing applications (the “Consumer IoT”), as distinct from industrial, commercial, and enterprise applications. Consumer applications represent less than one-third of the IoT’s potential economic value.¹³ It is especially critical for policymakers to understand this distinction and ensure both categories of IoT development—consumer and industrial/commercial/enterprise—are not curbed by over-regulation. Further, policymakers must recognize that consumer data can provide broader public interest benefits, *e.g.*, using data from smart thermostats for grid management and traffic data from mobile phones for smart city development. In this vein, CTA applauds the recent creation of the bipartisan, congressional Internet of Things Working Group, which aims to educate Members and bring them “up to speed on this technology and its impact on the modern economy and consumers.”¹⁴

¹³ See James Manyika *et al.*, *Unlocking the potential of the Internet of Things*, McKinsey Global Institute (June 2015) (“Business-to-business applications will probably capture more value—nearly 70 percent of it—than consumer uses...” (“*Unlocking the Potential*”), <http://www.mckinsey.com/business-functions/business-technology/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world>.

¹⁴ Rep. Bob Latta (R-OH) and Rep. Peter Welch (D-VT), *The Internet of Things has the potential to be the engine that powers our economy for decades to come*, The Hill Congress Blog (May 31, 2016 9:01 AM), <http://thehill.com/blogs/congress-blog/technology/281495-the-internet-of-things-has-the-potential-to-be-the-engine-that>.

C. Current or Planned Laws, Regulations, and/or Policies that Apply to IoT (Question 3)

As observed in the RFC, the Department’s “long standing technological and policy expertise” can help foster the IoT and its related economic benefits.¹⁵ In addition, the Department’s U.S. Patent and Trademark Office (“USPTO”) can continue its efforts to improve “patent quality, especially in new technological domains, including IoT.”¹⁶ As more “things” become embedded with patentable technologies, the “attack surface” for patent assertion entities—better known as “patent trolls”—grows. Patent reform, enabled by Congress and implemented by the USPTO, aimed at blunting patent trolls will remove a harmful tax on IoT development. And, as discussed in more detail below, spectrum policy, privacy and cybersecurity, and international standards have the potential to encourage or hinder the IoT, making it important that the U.S. does this right.¹⁷

D. Technological Issues That May Hinder IoT Development (Question 6)

Interoperability and voluntary global standards. A certain level of standardization and interoperability is necessary to achieve a successful, IoT ecosystem. In the emerging IoT economy, voluntary global standards accelerate adoption, drive competition, and enable cost-effective introduction of new technologies. Open standards which facilitate interoperability across the IoT ecosystem will stimulate industry innovation and provide a clearer technology

¹⁵ RFC at 19,958; *see also id.* (noting the that the “Department’s National Institute of Standards and Technology (NIST) has coordinated the development of a draft reference architecture for Cyber-Physical Systems and is conducting a Global City Teams Challenge to foster the development of Smart Cities and promote interoperability, NTIA’s spectrum planning and management activities contemplate the growth of IoT, and its Institute for Telecommunications Sciences (ITS) has begun testing the possible effects of IoT on spectrum usage”); *id.* (“The mission of the Department is to help establish conditions that will enable the private sector to grow the economy, innovate, and create jobs.”).

¹⁶ RFC at 19,958.

¹⁷ *See* Sections II.I and II.J, *infra*, discussing several current initiatives that apply to IoT. Similarly, as noted in Section II.F, the recently enacted FAST Act can encourage the development and development of transportation-related IoT applications.

evolution path. To the extent that interoperability and reliability are related, enabling manufacturers and consumers to create a feedback loop will better calibrate end-user expectations and lead to more useful, cheaper IoT applications, than any government mandate.

Industry is in the best position to develop the technological standards and solutions to address global IoT ecosystem opportunities and challenges. Government should encourage industry to collaborate in open participation global standardization efforts like the Industry Internet Consortium and Open Connectivity Foundation to develop technological best practices and standards.¹⁸ Specifically, government should encourage—not but mandate—the use of commercially available solutions to accelerate innovation and adoption of IoT deployments. Nor should the government mandate security standards. Consumer trust is critical for the IoT to succeed, and companies thus have a built-in incentive to protect data collected and used by IoT devices. The emphasis on commercially available solutions and market-adopted voluntary standards will allow for faster adoption and increase innovation, bringing the IoT and its benefits to reality sooner.

Spectrum availability and potential congestion/interference. Improved access to spectrum is critical to fueling the IoT. To connect the 50 billion devices that will be in use by 2020, a network would require capacity that is “at least 1,000 times the capability that exists today.”¹⁹ With the IoT showing promise in so many sectors of our economy, a broad range of

¹⁸ See About Us, Industry Internet Consortium, (“The Industrial Internet Consortium was founded in March 2014 to bring together the organizations and technologies necessary to accelerate the growth of the Industrial Internet by identifying, assembling and promoting best practices. Membership includes small and large technology innovators, vertical market leaders, researchers, universities and government organizations.”), <http://www.iiconsortium.org>; OCF-About, Open Connectivity Foundation (“The Open Connectivity Foundation (OCF) is creating a specification and sponsoring an open source project to make this possible.... OCF will help ensure secure interoperability for consumers, business, and industry.”), <http://openconnectivity.org>.

¹⁹ Murray Slovick, *5G: The Mobile Tech of 2020*, CTA i³, 20 (Nov./Dec. 2014), <http://cdn.coverstand.com/25838/232265/711ba5485b2b1c66036f89c895b2-baecbaa98e91.23.pdf>.

agencies must partner among themselves and with industry to ensure sufficient spectrum to match the needs of the IoT. The wide variety of IoT spectrum uses means that the Department's National Telecommunications and Information Administration ("NTIA") must help facilitate sharing and/or clearing of federally-controlled spectrum. Given the cross-cutting nature of IoT, agencies must collaborate to enable the IoT to flourish. The joint letter signed by the leaders of the FCC, Department of Transportation ("DOT"), and the Department committing to a testing plan for shared uses in the 5.9 GHz band, is an interagency collaboration that could help, should the agencies follow through on this commitment.²⁰ If successful, it could be replicated elsewhere, as well as demonstrate a commitment to the consultation advice of industry.

Recognizing that the federal government is the largest single holder of spectrum in the country, federal agencies must share, and where possible clear, spectrum "to ensure the IoT industry has access to the spectrum it needs to continue to grow and change our lives for the better."²¹ Public statements recognizing the importance of spectrum and the IoT are starting to

²⁰ Letter from Penny Pritzker, Sec'y, Dep't of Commerce, Anthony Foxx, Sec'y, Dep't of Transp., and Tom Wheeler, Chairman, Fed. Commc'ns Comm'n, to John Thune, Chairman, Senate Committee on Commerce, Sci., and Transp. (Jan. 2016), <http://src.bna.com/bZt>.

²¹ Press Release, CTA, *Future IoT Success Depends on Access to Spectrum, CTA Says* (Mar. 3, 2016), <http://www.cta.tech/News/News-Releases/Press-Releases/2016-Press-Releases/Future-IoT-Success-Depends-on-Access-to-Spectrum.aspx> (quoting CTA President and CEO Gary Shapiro in support of the Developing Innovation and Growing the Internet of Things Act).

build support for agency action.²² Even some of the bills currently pending before Congress have the potential to increase available spectrum for commercial uses, including the IoT.²³

NTIA should also keep in mind the wide range of use cases, and fitting for such a wide range, adopt a technologically neutral approach to the IoT policy framework. The incredible variety of applications in consumer, industrial, commercial, and enterprise spaces means that different kinds of spectrum will be suitable in different situations, including those delivered by wireline, wireless, and satellite. Lower frequencies will be important for coverage and distance in some applications; higher frequencies will also have their value and applicability for IoT. By not favoring any single technology, NTIA can encourage the growth of IoT services across platforms, which will ensure that the best technology is available for each existing and future use case.

E. Factors the Department and Government More Generally Should Consider When Prioritizing Technical Activities with Regard to IoT (Question 7)

The NTIA and the National Institute of Standards and Technology (“NIST”) must continue important research into how spectrum can be shared and measured.²⁴ NIST’s cybersecurity framework—the research underlying the framework and the private-public

²² See, e.g., Cory Booker, Kelly Ayotte, Brian Schatz, and Deb Fischer, *Policymakers Must Look Ahead to Realize the Potential of the Internet of Things*, CTA i³ (Mar. 10, 2016), <http://www.cta.tech/i3/Move/2016/March-April/Policymakers-Must-Look-Ahead-to-Realize-the-Potent.aspx>; Bob Latta and Michael O’Rielly, *Improving the 5.9 GHz Band to Enhance Unlicensed and Wi-Fi Networks*, The Hill: Congress Blog (Mar. 2, 2016, 9:00 AM), <http://thehill.com/blogs/congress-blog/technology/271408-improving-the-59-ghz-band-to-enhance-unlicensed-and-wi-fi>.

²³ See, e.g., Developing Innovation and Growing the Internet of Things Act, S. 2607, 114th Cong. (2016); MOBILE NOW Act, S. 2555, 114th Cong. (2016); Wi-Fi Innovation Act, H.R. 821 and S. 424, 114th Cong. (2016).

²⁴ In particular, NTIA has been responsive to the recommendations of the Commerce Spectrum Management Advisory Committee (“CSMAC”) with respect to industry-government collaboration and spectrum sharing. Paige R. Atkins, Assoc. Adm’r, Nat’l Telecomm. and Info. Admin., *CSMAC Recommendations: NTIA Preliminary Response* (Dec. 2, 2015) (observing that many of CSMAC’s recommended actions are already initiated or are a part of on-going NTIA activities), <http://1.usa.gov/20yhS2j>.

collaboration as the framework developed—is an example of a beneficial technical activity that should be replicated with respect to IoT. As discussed above, given that the numerous IoT technologies will vary depending on IoT use case—from Bluetooth to Wi-Fi to Cellular to Ethernet—it would not make sense to allocate “IoT spectrum.” The best enabler is to generally and flexibly open up new licensed and unlicensed spectrum to accommodate any and all communications technologies that may be needed for foreseeable and non-foreseeable IoT use cases.

F. Role of Government in Bolstering and Protecting Availability and Resiliency of Infrastructures to Support IoT (Question 10)

The Department correctly observed that “infrastructure investment, innovation, and resiliency (such as across the information technology, communications, and energy sectors) will provide a foundation for the rapid growth of IoT services.”²⁵ CTA’s members are investing heavily in next generation cellular (5G) and next generation Wi-Fi technologies and look forward to partnering with the public sector as part of the Administration’s Smart Cities Initiative, which will “invest over \$160 million in federal research” to leverage IoT “to improve the life of ... residents.”²⁶ Similarly, CTA is closely following DOT action in response to the recently enacted FAST Act.²⁷ The FAST Act rightfully permits the DOT greater flexibility with respect to various surface transportation funding allocations and programs to be used on

²⁵ RFC at 19,959.

²⁶ Press Release, The White House, *FACT SHEET: Administration Announces New “Smart Cities” Initiative to Help Communities Tackle Local Challenges and Improve City Services* (Sept. 14, 2015), <http://1.usa.gov/1MttsZD>. The new capabilities and services made possible by the IoT require advancement and investment in our current infrastructures in order to securely deliver, grow, and scale adoption. Our current networks do not have the capacity to transmit, secure, or store the explosion of data that is being generated by the fifty billion estimated devices connecting by 2020.

²⁷ Fixing America’s Surface Transportation Act, Pub. L. No. 114-94, 129 STAT. 1312, (2015).

technology deployment, including Intelligent Transportation System technologies and other applications of the IoT.²⁸

The government has played a critical role in building infrastructure in other contexts. For example, to promote broadband deployment as a high priority, President Obama issued Executive Order (“E.O.”) No. 13616, “Accelerating Broadband Infrastructure Deployment,”²⁹ to facilitate wired and wireless broadband infrastructure deployment in federal lands and buildings. Among other things, the E.O. established a working group comprised of representatives from fourteen federal agencies and offices, whose task was to ensure a coordinated approach in implementing agency procedures, requirements, and policy with respect to broadband deployment on federal lands and buildings. In one short year, the working group made a number of process and policy improvements designed to promote broadband deployment, including coordinating consistent and efficient federal broadband procedures, coordinating use of uniform contracts and applications, and establishing best practices for excavations for the installation of broadband facilities during federal or federally assisted highway construction.³⁰

Likewise, President Obama on March 23, 2015 signed a Presidential Memorandum³¹ creating the Broadband Opportunity Council (“Council”), co-chaired by the departments of Commerce and Agriculture and comprised of twenty-five federal agencies and departments, to “engage with industry and other stakeholders to understand ways the Executive Branch can

²⁸ CTA also eagerly anticipates the DOT report on the “Potential of the Internet of Things,” which Congress directed the DOT to create by June 4, 2016. *Id.* § 3024, 129 Stat. at 1494.

²⁹ Exec. Order No. 13616, 77 Fed. Reg. 36903 (June 20, 2012), <http://1.usa.gov/1SNR1vy>.

³⁰ Broadband Deployment on Federal Property Working Group, *Implementing Executive Order 13616: Progress on Accelerating Broadband Infrastructure Deployment*, Progress Report to the Steering Committee on Federal Infrastructure Permitting and Review Process Improvement (Aug. 2013), <http://1.usa.gov/1O5MyqP>.

³¹ Memorandum on Expanding Broadband Deployment and Adoption by Addressing Regulatory Barriers and Encouraging Investment and Training, DCPD-201500195 (Mar. 23, 2015), <http://1.usa.gov/25yy7Ql>.

better support the needs of communities seeking broadband investment.”³² The White House released the Council’s report in 2015 outlining action items and milestones to be taken by each agency to remove barriers to broadband deployment.³³

By focusing on accelerating the buildout of broadband infrastructure on federal lands, the government led by example, catalyzing investment and innovation in the private sector and forging many innovative public/private partnerships.³⁴ It can and should play a similar role here with respect to the deployment of infrastructure necessary to advance IoT technologies.

G. How Government Should Quantify and Measure the IoT Sector (Question 11); How Government Should Measure the Economic Impact of IoT (Question 12)

Our projections show that in 2016 alone, IoT applications will drive the consumer technology industry to \$287 billion in retail revenues.³⁵ IoT also has significant potential to save consumers money and reduce residential energy consumption.³⁶ Although estimates vary, they all foretell incredible potential.³⁷ For example, ABI research forecast that IoT-related value

³² NTIA, *Broadband Opportunity Council*, <http://1.usa.gov/1Uf2qUz>.

³³ Penny Pritzker and Tom Vilsack, Dept. of Commerce & U.S. Dept. of Agriculture, *Broadband Opportunity Council Report and Recommendations* (Aug. 20, 2015), <http://1.usa.gov/1JISS3V>.

³⁴ See e.g., NTIA, *Broadband Technology Opportunities Program (BTOP) Quarterly Program Status Report* (July 2015), <http://1.usa.gov/1t1JWRA>; NTIA, *BroadbandUSA: An introduction to effective public-private partnerships for broadband investments* (Jan. 2015), <http://1.usa.gov/1B7L9YD>.

³⁵ CTA, *U.S. Consumer Technology Sales and Forecasts* (Jan. 2016), <https://www.cta.tech/Research/Products-Services/Consumer-Sales-Forecast.aspx>.

³⁶ Press Release, CTA, *Home Automation, IoT Could Cut Energy Consumption 10 Percent, says CTA Study* (explaining that a recent study predicts that “widespread adoption of home automation products such as temperature, circuit and lighting control, if used for energy savings purposes, could collectively avoid up to 100 million tons of CO2 emissions and reduce total residential primary energy consumption by as much as 10 percent - that savings is more than consumer electronics' share of residential primary energy consumption (8.4 percent) according to a separate CTA study”).

³⁷ See, e.g., *Unlocking the Potential* (“If policy makers and businesses get it right, linking the physical and digital worlds could generate up to \$11.1 trillion a year in economic value by 2025.”); Louis Columbus, *Roundup Of Internet of Things Forecasts And Market Estimates, 2015*, *Forbes* (Dec. 27, 2015 3:39 PM) (surveying several IoT market forecasts), <http://onforb.es/1ZbLjXD>.

added services will grow from \$50 billion in 2012 to \$120 billion in 2018.³⁸ In a comprehensive study, Cisco predicted that the IoT will “create[] \$14.4 *trillion* in Value at Stake—the combination of increased revenues and lower costs that is created or will migrate among companies and industries from 2013 to 2022.”³⁹ Because IoT applications will become so entwined with everyday activity, the focus should be on the marginal benefit (and marginal cost) of IoT uses.

H. Impact of the Growth of IoT on the U.S. Workforce and Potential Benefits for Employees and/or Employers (Question 14)

Advances in the IoT, combined with general innovation-friendly policies, can help the U.S. maintain its role as a global leader in technology and unleash economic growth.⁴⁰ The U.S. technology sector is the strongest and most innovative in the world, and appropriate limited federal and state government action, as well as restraint, will ensure that the nation maintains its leadership in the burgeoning IoT market.⁴¹ However, this leadership is being challenged by other countries that are aggressively pursuing IoT transformation. For example, China has stated that “Made in China 2025”, the Chinese government’s blueprint for overhauling industry and rebranding China as a high-quality manufacturer, is based on smart manufacturing (a network of intelligent, connected factories), emphasizes innovation and quality, and includes US\$6.4 billion exclusively for China’s emerging industries.⁴² Additionally, Germany is actively pursuing Industrie 4.0, the German vision for the future of manufacturing, where smart factories use

³⁸ *Id.*

³⁹ Joseph Bradley, *Embracing the Internet of Everything To Capture Your Share of \$14.4 Trillion*, Cisco White Paper, at 1(2013), http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoE_Economy.pdf.

⁴⁰ See *infra* Section II.N discussing tax and immigration policies that can increase these benefits.

⁴¹ See Intel, *Policy Framework for the Internet of Things (IoT)* (2014) (describing the value to the U.S. economy of the U.S. tech sector taking a leading role in the global IoT market), <http://intel.ly/22okUYy>.

⁴² Ringier Metalworking, *Smart Manufacturing in China*, *industrysourcing* (Sept. 5, 2015 11:09:23 AM), <http://www.industrysourcing.com/article/smart-manufacturing-china>.

information and communications technologies to digitize their processes and reap huge benefits in the form of improved quality, lower costs, and increased efficiency.⁴³ As CTA has observed:

With some of the world's most disruptive companies - both global brands and innovative startups - the U.S. tech sector will help reduce the deficit, create jobs, improve sustainability and grow the economy. And tech's evolving sharing economy brings unique value, giving us more transportation and hospitality choices, creating good jobs with flexible hours and tapping capital resources such as a second car or a spare bedroom. But we must have the right policies in place to achieve tangible benefits.⁴⁴

I. How Government Should Address the Main IoT Policy Issues (Question 15)

The RFC observes that a “growing dependence on embedded devices in all aspects of life raises questions about the confidentiality of personal data, the integrity of operations, and the availability and resiliency of critical services.”⁴⁵ Yet while government has a critical role to play in ensuring that its policies enable industry to meet demand for IoT offerings, it must be sure to limit other types of regulatory intervention—and to forego entirely any actions that could stifle innovation in the nascent IoT ecosystem.⁴⁶ Prescriptive regulation, however well intentioned, could inadvertently deter the development and deployment of the IoT. Likewise, fragmented and, its flip-side, overlapping regulations are artificial hurdles that the Department should avoid. Specifically, policymakers at all levels of government should exercise regulatory humility, taking only actions consistent with the following core framework:

⁴³ Sara Zaske, *Germany's vision Industrie 4.0: The revolution will be digitized*, ZDNet (Feb. 23, 2015 08:33 GMT), <http://www.zdnet.com/article/germanys-vision-for-industrie-4-0-the-revolution-will-be-digitised>.

⁴⁴ Press Release, CTA, *Tech Innovation Key to President's SOTU Vision, Says Consumer Technology Association* (Jan. 12, 2016), <http://cta.tech/News/News-Releases/Press-Releases/2015-Press-Releases/Tech-Innovation-Key-to-President-s-SOTU-Vision.-sa.aspx>.

⁴⁵ RFC at 19,959.

⁴⁶ For example, the hands-off approach to Internet regulation launched massive innovation. The Department should replicate that approach with the IoT.

First, to promote innovation, policymakers should favor market-based solutions over prescriptive regulations. Government should apply regulation only if there is a compelling public interest in doing so.⁴⁷ Policymakers should not reflexively second-guess how consumers or businesses decide to incorporate technology into their lives. Likewise, in the rare event where policymakers believe that regulation would be superior to a market-based outcome, policymakers should test their assumption by applying empirical analyses to do a comprehensive cost-benefit analysis vis a vis alternative technologies, as well as determine whether the benefits of a proposed regulatory mandate will exceed its costs. Such cost-benefit analyses can help balance the need for consumer protection with the need to allow flexibility to innovate.⁴⁸ Independent industry data should play a key role in these decisions.

Second, the primary goal of any IoT policy regime should be to promote innovation. As President Barack Obama observed in his 2011 State of the Union address: “The first step in winning the future is encouraging American innovation.... [W]hat America does better than anyone else ... is spark the creativity and imagination of our people.... In America, innovation

⁴⁷ See Gary Shapiro, *How the Heavy Hand of Government Stifles the On Demand Economy*, TechDirt (Aug. 25, 2015) (“*The Heavy Hand of Government*”), <https://www.techdirt.com/articles/20150824/11370432049/how-heavy-hand-government-stifles-demand-economy.shtml>.

⁴⁸ For decades, Executive Branch agencies in the United States have been required to “(1) propose or adopt a regulation only upon a reasoned determination that its benefits justify its costs (recognizing that some benefits and costs are difficult to quantify); (2) tailor [their] regulations to impose the least burden on society, consistent with obtaining regulatory objectives, taking into account, among other things, and to the extent practicable, the costs of cumulative regulations; (3) select, in choosing among alternative regulatory approaches, those approaches that maximize net benefits (including potential economic, environmental, public health and safety, and other advantages; distributive impacts; and equity); (4) to the extent feasible, specify performance objectives, rather than specifying the behavior or manner of compliance that regulated entities must adopt; and (5) identify and assess available alternatives to direct regulation, including providing economic incentives to encourage the desired behavior, such as user fees or marketable permits, or providing information upon which choices can be made by the public.” See Exec. Order No. 13, 563, 76 Fed. Reg. 3,821 (Jan. 18, 2001) (summarizing Exec. Order No. 12,866, 58 Fed. Reg. 51,735 (Sept. 30, 1993)). President Obama enhanced these principles, directing agencies to, among other things, “identify and consider regulatory approaches that reduce burdens and maintain flexibility and freedom of choice for the public” where permitted by law.

doesn't just change our lives. It is how we make our living."⁴⁹ Further, "our free enterprise system is what drives innovation."⁵⁰

Third, if policymakers decide that some form of oversight is appropriate in a given case, they should proceed with caution, favoring self-regulation over command-and-control on determining how the outcomes are achieved. CTA and groups like it have long been committed to solutions that marry industry expertise, stakeholder involvement, and the flexibility required by a fast-changing marketplace. Standards ensure that technical issues are addressed in cooperative forums, principally by technologists rather than attorneys, and often eliminating any need for regulatory mandates. A wide variety of groups develop and enforce tailored industry codes of conduct that hold bad actors to account without undermining innovation.⁵¹

Consistent with these principles, policymakers should reject mandates that would distort the IoT's trajectory and undercut the growth of offerings that would expand consumers' welfare. In particular, they should reject actions that favor one platform or technology over another or create or expand uncertainty, and should foreswear excessively punitive enforcement penalties.⁵² In the case of the IoT, incorrect, unnecessary, or premature mandates have the potential to distort the marketplace in a way that may disadvantage the US on a globally competitive basis. They could delay, dis-incentivize or prevent the development of new and superior technologies that would do better to improve our health outcomes, energy conservation efforts, or highway safety (to take just three examples). While protection of consumers should always remain at the forefront of regulators' minds, government must refrain from over-reaching enforcement actions

⁴⁹ The White House, *Remarks by the President in State of Union Address* (Jan. 25, 2011), <http://1.usa.gov/1Uisr5d>.

⁵⁰ *Id.*

⁵¹ *See infra* Section II.J, responding to Questions 16-17.

⁵² *See The Heavy Hand of Government.*

that harm consumers by mandating a specific technology, increasing the cost of providing service or entering a sector without providing commensurate consumer benefit.

J. How Government Should Address IoT Cybersecurity and Privacy Concerns (Questions 16-17)

The Internet's growth is largely attributable to the success of consensus-driven stakeholder processes to address policy issues,⁵³ and the privacy and security concerns associated with the IoT closely mirror those in which industry already has a strong track record of developing and implementing best practices to protect consumers. To address cybersecurity and privacy concerns, government must continue to foster industry-wide, consensus-driven self-regulation that is nimble and keeps pace with rapidly evolving technologies.

Self-regulatory regimes have worked well to ensure consumer privacy and foster innovation. The use of consumer information for marketing and other purposes is not new, as marketers have engaged in responsible collection of data for more than 100 years.⁵⁴ Time and again, industry has proactively addressed emerging privacy and security issues.⁵⁵ In contrast,

⁵³ See, e.g., *Executive Office of the President of the United States, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, 23 (2012) (“the Administration believes that multistakeholder processes underlie many of the institutions responsible for the Internet’s success”), <http://1.usa.gov/1FQW1XF> (“Consumer Data Privacy Framework”).

⁵⁴ Susan Taplinger, *The Plain Facts: Why Self-Regulation Works Better than Government Regulation*, DMA (May 9, 2014), <http://thedma.org/blog/advocacy/the-plain-facts-why-self-regulation-works-better-than-government-regulation>.

⁵⁵ Efforts of organizations like the Digital Advertising Alliance and Network Advertising Initiative have provided robust protections and tools to consumers as they use the Internet. See, e.g., *Consumer Data Privacy Framework, supra*, at 12-13 (citing AboutAds.info, *Self-Regulatory Principles for Online Behavioral Advertising* (July 2009)) (“[P]rompted by the FTC, members of the online advertising industry developed self-regulatory principles based on the FIPPs, a common interface to alert consumers of the presence of third party ads and to direct them to more information about the relevant ad network, and a common mechanism to allow consumers to opt out of targeted advertising by individual ad networks.”), <http://www.aboutads.info/resource/download/seven-principles-07-01-09.pdf>; Edith Ramirez, Chairwoman, FTC, *Cross-Device Tracking: An FTC Workshop*, 6-7 (Nov. 16, 2015) (“The Digital Advertising Alliance and the Network Advertising Initiative have also taken steps to enhance privacy protections in the online advertising space. The organizations’ self-regulatory principles encourage

unnecessary government action can skew or suppress innovation, create market uncertainty, and ultimately harm consumers. Legislation and regulation often fail to keep up with ever-evolving technology, and often rely—to the detriment of the marketplace and consumers—on regulators’ static assumptions and predictions of where the market is going and what consumers want. Self-regulation is nimble, and can be more easily updated to address changes in the marketplace and technology. And self-regulatory efforts push companies to “internalize ethical behavior and principles since the rules are based on social norms and conduct of peers rather than top-down prescriptive rules.”⁵⁶ In fact, self-regulatory codes may be the *best* way to effectuate consumer adoption of the IoT.⁵⁷ As a backstop with respect to consumer privacy, the FTC can utilize its Section 5 authority to protect against any privacy-related practices that are unfair or deceptive.⁵⁸

As a general matter, the increasing number of devices should not automatically trigger new regulations—before acting, there should be evidence of real harms. As IoT standards and technology continue to develop, regulatory efforts should be designed to promote innovation and

members to provide increased transparency and offer consumers control over data collection for certain practices. DAA and NAI also have developed useful opt-out tools for online data collection covered by their self-regulatory codes. NAI has also issued guidance relating to the use of non-cookie technologies, emphasizing that members should honor user opt-outs regardless of the technology used. NAI is currently developing and testing a new centralized opt-out tool that will inform consumers when NAI members use non-cookie technologies for interest-based advertising.”), <http://1.usa.gov/1XvgbU6>.

⁵⁶ Daniel Castro, *Benefits and Limitations of Industry Self-Regulation for Online Behavioral Advertising*, The Information Technology & Innovation Foundation, 6 (Dec. 2011), <http://www.itif.org/files/2011-self-regulation-online-behavioral-advertising.pdf>.

⁵⁷ Christopher Wolf and Jules Polonetsky, *An Updated Privacy Paradigm for the “Internet of Things”*, The Future of Privacy Forum, 11 (Nov. 19, 2013) (“As the Internet of Things becomes more ubiquitous, parents will want to control what can be done with information collected from devices associated with their children. Others may want to indicate their preferences about how third-party connected devices will communicate with them. Self-regulatory codes of conduct will be the most effective means to honor these preferences and others in the rapidly evolving landscape of the Internet of Things.”), <https://fpf.org/wp-content/uploads/Wolf-and-Polonetsky-An-Updated-Privacy-Paradigm-for-the-%E2%80%9CInternet-of-Things%E2%80%9D-11-19-2013.pdf>.

⁵⁸ In addition the FTC action, the Department should note that regulations already exist and apply to IoT with respect to privacy, data security, energy, finance, and transportation.

realize the potential value in this emerging industry. Further, if there are new regulations, they will have to be harmonized with existing regulations; there will need to be further harmonization if state and federal agencies enact rules. A fragmented regulatory environment will limit innovation and growth of this industry.

Moreover, the Department should note that stakeholders already are proactively addressing IoT privacy concerns.⁵⁹ In addition, CTA and its members participate in a number of other ongoing efforts to address a host of IoT issues, including those convened by think tanks, other associations, and the Administration.⁶⁰ Other examples include:

- The Future of Privacy Forum’s discussion document on privacy principles for facial recognition technology;⁶¹
- The President’s National Security Telecommunications Advisory Committee (“NSTAC”), with the mission to provide the U.S. Government the best possible industry advice in areas of national security;⁶²

⁵⁹ For example, 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 technology companies. Among other things, the Guiding Principles recommend that companies: provide robust security measures; provide clear, concise, and transparent information on the use of data collection, storing, and sharing, especially when transferring data to unaffiliated third parties; allow consumers the ability to control and review their personal wellness data; offer users the ability to opt out of advertising; and disclose their protocol for responding to law enforcement requests. See CTA, *Guiding Principles on the Privacy and Security of Personal Wellness Data*, <http://www.cta.tech/healthprivacy>; CTA, *Association Unveils First-of-Its-Kind, Industry Supported Principles on Wellness Data Privacy* (Oct. 26, 2015), <https://www.cta.tech/News/News-Releases/Press-Releases/2015-Press-Releases/Association-Unveils-First-of-Its-Kind,-Industry-Su.aspx>. CTA intends to review the Guiding Principles with members on a regular basis to ensure that the Principles accurately reflect current data privacy and security concerns.

⁶⁰ For example, the National Cyber Security Alliance and the WiFi Alliance, both of which share some members with CTA, have developed the following resources: <http://www.StaySafeOnline.org> and <http://www.wi-fi.org/discover-and-learn/security>.

⁶¹ The Future of Privacy Forum, *Privacy Principles for Facial Recognition Technology* (Dec. 2015), <https://fpf.org/wp-content/uploads/2015/12/Dec9Working-Paper-FacialRecognitionPrivacyPrinciples-For-Web.pdf>.

⁶² See Department of Homeland Security, *About NSTAC*, <https://www.dhs.gov/about-nstac>.

- The Alliance of Automobile Manufacturers and the Association of Global Automakers' initiative to establish privacy principles;⁶³
- The Automotive Security Review Board initiative to codify best practices and design recommendations for advanced cybersecurity solutions and products to benefit the automobile industry and drivers;⁶⁴
- The Online Trust Alliance's IoT Trust Framework, which currently includes practices to address security, privacy, and sustainability concerns in connected home products and consumer-facing wearable technologies;⁶⁵ and
- The NTIA's multistakeholder process to develop privacy, transparency, and accountability best practices for unmanned aircraft system use.⁶⁶

K. Ways that the IoT Affects and is Affected by Questions of Economic Equity (Question 19)

In addition to improving government services and increasing industrial efficiency, IoT applications have the potential to provide critical services for all Americans, including members of “disadvantaged communities and groups” and rural communities.⁶⁷ For example, CTA's research demonstrates that the IoT applications can “prevent and preempt life inconveniences caused by ... aging challenges.”⁶⁸ As the aging population increases, institutional long-term care services cannot meet demand and, even if they could, many seniors want to age in their homes for as long as possible.⁶⁹ Emerging applications include safety monitoring that can prevent

⁶³ The Alliance of Automobile Manufacturers, *Automotive Privacy: Automakers Believe that Strong Consumer Data Privacy Protections are Essential to Maintaining the Trust of Our Customers*, <http://www.autoalliance.org/auto-issues/automotive-privacy>.

⁶⁴ The Automotive Security Review Board, <https://newsroom.intel.com/news-releases/intel-commits-to-mitigating-automotive-cybersecurity-risks>.

⁶⁵ Online Trust Alliance, *Internet of Things*, <https://otalliance.org/initiatives/internet-things>.

⁶⁶ NTIA, *Multistakeholder Process: Unmanned Aircraft Systems*, <http://1.usa.gov/1KQNZYy>.

⁶⁷ RFC at 19,959 (“In what ways could IoT potentially help disadvantaged communities or groups? Rural communities?”).

⁶⁸ Consumer Technology Association Foundation and CTA, *Active Aging Study*, Report, at 6 (Mar. 2016).

⁶⁹ *Id.* at 66-68; Steven Ewell, *Smart Homes for Long Lives*, CTA i³, at 46 (Sept./Oct. 2015) (also noting that programs, such as the CTA Foundation-supported Selfhelp Virtual Senior Center, is “using technology to reconnect homebound seniors”), <http://mydigimag.rrd.com/publication/?i=272619&p=48>.

seniors from getting lost, improved living comfort through smart sensors and controls, and health monitoring can help seniors stay in their homes longer by making homes a little friendlier and reducing the time caregivers and even medical professionals need to spend on-site.⁷⁰ CTA Foundation proudly supports the Older Adults Technology Services’ (“OATS”) Senior Planet Exploration Center in New York, among many other initiatives, which offers classes and sits down with seniors to explain technologies, demystifying and unlocking technology.⁷¹

Similarly, individuals with disabilities—including many seniors—are harnessing the IoT to live safer, more independent lives:

While many drivers dream about being able to sit back and relax during a long commute, [self-driving cars] can literally open a new world to those who are physically unable to drive, providing access to daily routines such as grocery shopping or visiting friends and family, as well as bigger opportunities like facilitating steady employment and accessing health care.⁷²

For those with physical limitations, controlling lights and thermostats can transform a dwelling into a comfortable home.⁷³ IoT applications convert signals delivered aurally—think a doorbell and telephone ring—into signals delivered into visually or physical—flashing lights and

⁷⁰ *Id.* at 6.

⁷¹ *See, e.g.*, CTA Foundation, Initiatives (“CTA Foundation Initiatives”), <http://www.cta.tech/Foundation/Initiatives.aspx>; *see also* CTA Foundation Initiatives (quoting a Senior Planet member, “This week I was awarded my 100th Elance job! I have retained my five-star average, and now have six repeat clients, and my latest ranking as of last week is No. 76 out of the 239,000 writers registered with the site worldwide. Prior to my OATS training, I had never even heard of Elance, but through your classes I gained the skills and confidence to give it a try.”).

⁷² CTA, *2015 Sustainability Report: Innovating a Better World*, at 44 (2015) (“*Innovating a Better World*”), http://content.ce.org/SReport2016/CTA_SR_2016/report-builder/pdf/CTA_2015_SR.pdf.

⁷³ *See, e.g.*, Shalene Gupta, *For the disabled, smart homes are home sweet home*, *Fortune* (Feb. 1, 2015 6:00 AM EDT) (“For years, [Steve O’Hear, who uses an electrical wheelchair,] had to rely on someone else to turn the lights on—that is until he installed Internet-connected lights that he could turn on with his smartphone.”), <http://fortune.com/2015/02/01/disabled-smart-homes>.

vibrating phones.⁷⁴ And, for individuals with cognitive disabilities, sensors can remind individuals to perform daily tasks or alert remote caregivers about a delayed routine task.⁷⁵ Importantly, many Consumer IoT applications are able to interface through smartphones, tablets, and other mobile devices, which have built in accessibility features for app designers and consumers to use. Finally, IoT-powered efficiency gains can lead directly to lower utility bills. A private-public partnership to ensure these communities have access to IoT devices can spur these benefits.

L. Factors and Issues the Department Should Consider in its International Engagement (Questions 20-23)

CTA commends the NTIA for separately soliciting comment in preparation for the upcoming 2016 World Telecommunications Standardization Assembly.⁷⁶ The Department should continue to solicit public comment on government positions in international standards fora.⁷⁷ With an extensive Technology and Standards program that includes more than 70 committees, subcommittees and working groups and roughly 1,100 participants as well as American National Standards Institute accreditation, CTA is a champion of voluntary, consensus-based standards. To that end, the Department, including NIST and NTIA, should promote international harmonization of standards. However, that harmonization should not be in the form of mandates from international fora. Further, the Department should continue to

⁷⁴ In particular, the CTA Foundation is partnering with the Gallaudet University Technology Access Program to use IoT to enable alerts for people are deaf or hard of hearing.

⁷⁵ *Innovating a Better World* at 44.

⁷⁶ *Input on Proposals and Positions for 2016 World Telecommunications Standardization Assembly*, Request for Public Comment, Docket No. 160509408-6408-01, RIN 0660-XC026, 81 Fed. Reg. 30518 (May 17, 2016) (“WTSA-2016 RFC”). CTA looks forward to commenting on the WTSA-2016 RFC.

⁷⁷ RFC at 19,958 (“Both NIST and NTIA have been actively engaged with international standards bodies and international organizations on aspects of IoT and other related areas (e.g., cybersecurity), and have been further engaged with other Federal agencies.”).

promote regulatory harmonization to increase economics of scales. Consumers and society benefit when CTA's members are able to design, build, and test *once* and sell *everywhere*.

M. IoT Policy Areas that Could be Appropriate for Multistakeholder Engagement; Role the Department of Commerce Should Play in Addressing IoT Challenges and Opportunities and Collaborating with Stakeholders; Government and Private Sector Collaboration to Ensure that Infrastructure, Policy, Technology, and Investment are Working Together to Fuel IoT Growth and Development (Questions 25-27)

Building a strong public sector/private sector partnership can help bolster the foundation for consumer confidence and trust in the IoT. Government can advance the IoT by working with industry to develop a system of trust between users and connected things. Together government and industry can work to educate consumers on issues such as how to limit risks associated with unsecured connected devices (*e.g.*, by changing default passwords, using password-protecting home Wi-Fi networks, and employing virtual private networks).⁷⁸

The public/private partnership that has coalesced around the Department's recent cybersecurity initiatives is particularly illustrative. Most notably, various critical infrastructure sectors came together to develop the NIST Cybersecurity Framework, a voluntary, flexible, and non-regulatory approach that enables companies of all types and sizes to tailor their cybersecurity efforts to meet their business models, infrastructure, and assets.⁷⁹ Similar

⁷⁸ One example of this is the FTC's groundbreaking "Start with Security" series, where the FTC has taken business guidance on the road to San Francisco, Seattle, and Austin, to meet with startups, experts, and agency officials to discuss effective data security strategies.

⁷⁹ *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0, NIST, 1 (Feb. 12, 2014) (explaining that the "[f]ramework, created through collaboration between government and the private sector, uses a common language to address and manage cybersecurity risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses"), <http://1.usa.gov/1dIqXf5>. In response to requests for comment by NIST, industry recently voiced continued support of the Cybersecurity Framework as companies work through the early phases of building it into their risk management processes. *See Views on the Framework for Improving Critical Infrastructure Cybersecurity*, 80 Fed. Reg. 76,934 (Dec. 11, 2015).

business-led collaboration continues through other established mechanisms.⁸⁰ Additional industry coordination is facilitated through the Communications Security, Reliability and Interoperability Council (“CSRIC”)—an advisory committee to the FCC that recommends best practices and potential actions to ensure optimal security, reliability, and interoperability of commercial and public safety communications systems.⁸¹ Concurrently, NTIA has used its multistakeholder processes to further catalyze industry discussion on the cybersecurity-related issues, with the stated goal of avoiding regulatory solutions.⁸² Of course, all of these efforts parallel industry’s own initiatives, such as the Building Security in Maturity Model (“BSIMM”)—a study of actual software security initiatives that likewise is not a one-size-fits-all prescription.⁸³ In short, cybersecurity issues are being addressed in a multi-layered fashion, with industry consistently taking a lead in shaping the discussion. A similar approach to challenges posed by the growth of the IoT would ensure protection of consumers’ safety and quality of

⁸⁰ See, e.g., *About CSCC*, U.S. Communc’ns Sector Coordinating Council, (describing means of coordination used by the Communications Sector Coordinating Council), <http://www.commscc.org/about>. Sector Coordinating Councils formed for each of sixteen critical infrastructure sectors.

⁸¹ See *The Communications Security, Reliability and Interoperability Council*, FCC, <http://transition.fcc.gov/pshs/advisory/csric>. CSRIC’s working groups have proposed implementation guidance to help communications companies implement the NIST Cybersecurity Framework and continue to recommend and refine best practices in this space. *Cybersecurity Risk Management and Best Practices, Working Group 4: Final Report*, CSRIC IV (Mar. 2015), https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.

⁸² See, e.g., *Stakeholder Engagement on Cybersecurity in the Digital Ecosystem*, 80 Fed. Reg. 14,360, 14,363 (Mar. 19, 2015) (recognizing that traditional regulation in this context is “difficult and inefficient” in light of the “pace of innovation in the highly dynamic digital ecosystem”); *id.* at 14,365 (stating that “[i]n the digital ecosystem, the rapid pace of innovation often outstrips the ability of regulators to effectively administer key policy questions,” and that “[o]pen, voluntary, and consensus-driven processes can work to safeguard the interests of all stakeholders while still allowing the digital economy to thrive”); Angela Simpson, Deputy Assistant Sec’y of Commerce for Commc’ns and Info., Nat’l Telecomm. & Info. Admin., Remarks at the Vulnerability Research Disclosure Multistakeholder Process (Sept. 29, 2015) (“it is not our job to tell you what to do. NTIA will not impose its views on you. We will not tip the scales. We are not regulators. We are not developing rules. We do not bring enforcement actions. Instead, we are in a unique position to encourage you to come together, to cooperate, and to reach agreement on important issues.”), <http://1.usa.gov/1XvgMFd>.

⁸³ *About BSIMM*, Building Security in Maturity Model, <https://www.bsimm.com/about>.

service, while affording industry the opportunity to directly participate and shape parameters that can evolve flexibly as new business and technological developments emerge.

N. Additional Relevant Issues (Question 28)

The government can take additional steps toward ensuring that the U.S. IoT ecosystem maintains its global leadership role. For example:

Demand Stimulation. The government can generate demand for IoT technologies, which will help jumpstart the development of the IoT ecosystem. Agencies can utilize IoT technology themselves to increase efficiency in their management of public infrastructure and also can incent or require regulated utilities to use IoT technologies to more efficiently manage and conserve regulated resources such as energy and water.⁸⁴ This will result in direct and immediate benefits to the American public while simultaneously stimulating the IoT markets that supply the government and public utilities. By making the data collected by government-operated IoT systems available to industry (subject to appropriate privacy safeguards), governments can enable private companies to independently develop innovative new market niches. Through private-public partnerships, governments can empower private companies to develop new and better ways for governments to utilize IoT-generated data to provide more efficient and desirable public services.

Tax. Tax policy can help facilitate the rapid growth of the IoT sector, as exemplified by recent federal legislation making permanent certain previously temporary research and development (“R and D”) tax credits. Federal and state R and D tax credits reduce the risk to companies of investment in basic and applied R and D. Reduced risk fosters greater investment, which in turn spurs the type of rapid technological advancement that is predicted for the IoT

⁸⁴ See, e.g., *supra* Section II.F (discussing the Smart Cities Initiative).

sector over the next decade. The U.S. government took a strong step in the right direction when it expanded and made permanent the federal R and D tax credit in December 2015.⁸⁵ However, there remains room for improvement. In addition, more attention needs to be given to the unintended consequences of tax policies on the IoT market. Tax laws should foster IoT innovation rather than providing disincentives to the continued rapid deployment of the IoT, which should be driven by competition and consumer demand.

Immigration. Appropriate immigration policies are key to unleashing the potential of the IoT sector. In light of the breathtaking growth expected in this sector over the next decade, it is unlikely that the U.S.'s science, technology, engineering, and math ("STEM") work force will be sufficient to support the sector's rapid expansion⁸⁶ unless Congress adopts meaningful reform to the U.S.'s overly restrictive immigration policies. Strategic immigration reforms are needed to encourage U.S.-educated immigrants to remain in the U.S. to build businesses and create domestic jobs, and U.S. immigration policy should proactively promote their participation.

⁸⁵ Consolidated Appropriations Act, P.L. 114-113 § 1, 114th Cong. (2015) (Protecting Americans From Tax Hikes Act of 2015 was consolidated with the Military Construction and Veterans Affairs and Related Agencies Appropriations Act, H.R. 2029 (2016)). The PATH Act made permanent the R and D tax credit that initially was established in 1981 and that has expired and been renewed more than a dozen times since then. The law provides companies with a tax credit of up to 20% of their qualifying research expenditures. The PATH Act also enacted changes to the application of the credit, which increased its effective availability to small and medium-sized businesses. *Id.*

⁸⁶ Adams B. Nager and Robert D. Atkinson, *Debunking the Top Ten Arguments Against High-Skilled Immigration*, Information Technology & Innovation Foundation (Apr. 2015), http://www2.itif.org/2015-debunking-myths-high-skilled.pdf?_ga=1.42898860.847894678.1456315207.

III. CONCLUSION

The U.S. has a chance to harness the opportunities of the IoT to bring significant consumer, business, and societal benefits to the nation and solidify our global leadership in technology innovation and deployment. Policymakers should aggressively accelerate the positive steps government can take to promote IoT innovation, growth, and deployment, such as making more spectrum available and harmonizing federal agency interaction, and refrain from broad regulatory action that would derail or delay new IoT technologies. Self-regulatory and other consensus-driven industry efforts allow stakeholders to address discrete, specialized issues that may arise in a practical and flexible manner and without the same risks to competition and innovation—and these should be the default institutional mechanism for the IoT. For the IoT to flourish generally—and for new, never-thought-of-before IoT applications to positively impact and improve our lives—government must partner with industry to eliminate barriers to innovation, exercise regulatory humility by considering any regulatory actions in light of greater economic impacts, and embrace industry self-regulatory efforts that can address concerns as they arise without inhibiting innovation.

Respectfully submitted,

CONSUMER TECHNOLOGY
ASSOCIATION F/K/A CONSUMER
ELECTRONICS ASSOCIATION

By: /s/ Julie M. Kearney

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

June 2, 2016

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.

**Comments of the Consumer Electronics Association
to the
United States Federal Trade Commission
Patent Assertion Entity Reports: Paperwork Comment**
Project No. P13203
December 16, 2013

I. Introduction

The Consumer Electronics Association (“CEA”) is pleased to submit comments to the Federal Trade Commission (“FTC”) regarding the FTC’s proposed information requests to Patent Assertion Entities (“PAEs”) and other entities asserting patents in the wireless communications sector.¹ As the principal U.S. trade association of the consumer electronics and information technologies industries, with more than 2,000 member companies, CEA’s members are among the most innovative and creative in the world, and many of their remarkable repertoire of products use the patent protections afforded by U.S. law.² With increasing frequency, however, the PAEs that exist only to acquire patents, have twisted patent law and exploited imperfections in the patent system causing great damage to innovators and entrepreneurs. The routine filing of frivolous patent lawsuits by PAEs has diverted critical resources away from new product development and into costly litigation expenses; ultimately, this cold reality works to discourage the very same risk-taking that led to the development of so many of our most beloved consumer electronics products.

The FTC’s information requests are a necessary first step into quantifying the costs and benefits of PAE activity and only through the considered examination of PAEs’ and others’ data can the true negative effects of many PAEs’ activities be understood properly.³ The FTC – with its unique statutory mandate and authority under Section 6(b) of the Federal Trade Commission Act, 15 U.S.C. §46(b) to conduct such a Study⁴ – is well positioned to gather and analyze the broad array of data and information that will demonstrate this fact and lead to the necessary conclusion that status quo is untenable.

¹ Fed. Trade Comm’n, *Federal Register Notice Soliciting Public Comments On Proposed Information Requests To Patent Assertion Entities and Other Entities Asserting Patents In the Wireless Communications Sector, Including Manufacturers and Other Non-Practicing Entities and Organizations Engaged In Licensing*, available at <http://www.ftc.gov/os/fedreg/2013/09/130926paefrn.pdf> (visited Dec. 4, 2013) (hereinafter “Federal Register Notice”).

² See generally, Consumer Electronics Association, *About CEA*, available at <http://www.ce.org/About-CEA.aspx> (visited Dec. 4, 2013).

³ Chairwoman Edith Ramirez, *Remarks of Chairwoman Edith Ramirez, Fall Networking Event*, ABA Antitrust Section’s Intellectual Property Committee, Washington, DC, November 12, 2013, available at <http://ftc.gov/speeches/ramirez/131112eripcommittee.pdf>, at 3 (visited Dec. 4, 2013) (“Our aim is to use that authority to expand the empirical evidence on PAE activity and shed light on its likely costs and benefits.”)

⁴ Press Release, *FTC Seeks to Examine Patent Assertion Entities and Their Impact on Innovation, Competition* (Sept. 26, 2013), available at <http://www.ftc.gov/opa/2013/09/paestudy.shtm>.

The FTC has invited comment on four topics. CEA will limit its comments to the single topic on which CEA, as a trade association, is in best position to explore, “whether the proposed collection of information is necessary for the proper performance of the functions of the FTC, including whether the information will have practical utility.”⁵

II. The Proposed Collection of Information is Necessary for the Proper Performance of the Functions of the FTC, and this Information Will Have Practical Utility

a. The Proposed Collection of Information is Necessary for the Proper Performance of Functions of the FTC

The FTC is a law enforcement agency with authority to determine whether anticompetitive conduct is occurring in violation of the Sherman, Clayton, and Federal Trade Commission Acts.⁶ Each of these statutes, while distinct in verbiage and scope, share the same purpose: to ensure that conduct harmful to the proper functioning of competitive markets is prevented. It is unlikely that the drafters of those statutes could have imagined commerce like we see today, marked by rapid technological innovation and constant change. Yet the core competencies of these statutes still provide the FTC with the necessary flexibility to examine even modern-day developments like PAEs’ ability to abuse the patent system to anticompetitive ends.

This is not to suggest that all PAE activity is presumptively unlawful. Yet because PAEs’ activity can be uniquely and dramatically harmful, empirical study and close scrutiny is required. Thus, without sufficient detail, the FTC 6(b) Study cannot serve to explore and explain the actual anticompetitive consequences resulting from PAEs’ actions. The list of data the FTC must gather must be necessarily broad and incredibly detailed. Only by requesting quantification from PAEs regarding demand letters, litigation costs, and license information, among other items, as the information requests do, will provide the necessarily depth to assess meaningfully PAEs’ overall anticompetitive effect.

The FTC’s 6(b) Study will enable the FTC (and other stakeholders, like Congress) to assess the ramifications of PAE conduct on competition as a whole. This analysis will result in better informed enforcement decisions by the FTC, private parties, and others. And, as a result, this will undoubtedly help the FTC in performance of its core function to enforce the antitrust and competition laws.

⁵ Federal Register Notice at 16.

⁶ See generally, Fed. Trade Comm’n Office of the General Counsel, *A Brief Overview of the Federal Trade Commission’s Investigative and Law Enforcement Authority*, Revised July 2008, available at http://www.ftc.gov/ogc/brfovrw.shtm#N_1_.

b. There is Practical Utility in Gathering this Information Because It May Quantify the Negative Effect PAEs' Conduct Has on Competition

In law review articles, speeches, and previous public forums, including a 2012 FTC and Department of Justice Antitrust Division Workshop on PAEs,⁷ many elaborated on the anticompetitive effects resulting from PAEs' conduct. We need not repeat those adverse effects in detail here. What bears repeating is that without the benefit of the detailed information in the 6(b) Study, the true depth of harm caused by the PAEs' activity cannot be confirmed and accurately quantified. For example, the instances where PAEs have improperly targeted small businesses or individuals who provide WiFi services or use a scanner and threatened to file suit could be far greater than what has been reported in the press.⁸ These small businesses and individuals may not have the wherewithal to determine whether the PAEs' claim is valid and may have chosen to settle under draconian non-disclosure agreements demanded by the PAEs, rather than enter into a costly litigation posture. Understanding the scope of these kinds of potentially unwarranted settlements is absolutely essential to assessing the effect of PAEs' conduct on the market.

Medium and large-sized businesses with more sophisticated understandings of the patent laws may be equally compelled to settle rather than litigate. As has been explained by others, the cost of discovery in a patent suit disproportionately falls on the defendant and not the plaintiff-PAE.⁹ This asymmetry in litigation costs creates perverse incentives on both sides and divorces the dispute from its substantive underpinnings, a result that benefits only the PAE. Moreover, some entities are choosing to outsource patent warfare by assigning rights to "patent privateers," or PAEs who will sue on their behalf and who structure the sales such that it is an end-around mechanism to target the original owner's downstream competitive rivals. Here, the original owner benefits indirectly if the PAE raises its rivals costs.¹⁰ This adds an additional layer of uncertainty and expense and is certainly worthy of detailed study. Understanding the cost – to the cent – of defending these patent suits will provide a sound basis on which to compute the monetary loss that defending unjustified PAE suits requires.

Perhaps more importantly, with the constant threat of PAE litigation, the incentives for individuals and companies to create new products are reduced. As has been explained by others

⁷ Fed. Trade Comm'n & U.S. Dep't of Justice, Patent Assertion Entity Activities Workshop (Dec. 10, 2012), materials available at <http://www.ftc.gov/opp/workshops/pae/>.

⁸ This unfortunate phenomenon has been reported widely in the press. See, e.g., Joe Mullin, *Patent Trolls Want \$1,000—For Using Scanners* (Jan. 2, 2013), available at <http://arstechnica.com/tech-policy/2013/01/patent-trolls-want-1000-for-using-scanners/> (visited Dec. 4, 2013).

⁹ See, generally, e.g., U.S. Gov't Accountability Office, GAO-13-465, *Intellectual Property: Assessing Factors that Affect Patent Infringement Litigation Could Help Improve Patent Quality* (2013), available at <http://www.gao.gov/products/GAO-13-465>; and Sara Jeruss, Robin Feldman & Joshua Walker, *The America Invents Act 500: Effects of Patent Monetization Entities on US Litigation*, 11 DUKE TECH. L. REV. 357, 361 (2012).

¹⁰ Chairwoman Edith Ramirez, *Opening Remarks of Chairwoman Edith Ramirez, Competition Law & Patent Assertion Entities: What Antitrust Enforcers Can Do*, Computer & Communications Industry Association and American Antitrust Institute Program, Washington, DC (June 20, 2013), available at <http://www.ftc.gov/speeches/ramirez/130620paespeech.pdf> (visited Dec. 4, 2013).

and as we commented during the 2012 Workshop, this will lead to less creativity, less innovation and ultimately, less competition across products.¹¹

III. Conclusion

CEA applauds the FTC's efforts to assess the anticompetitive harms that PAEs cause on our economy as a whole. The information requests are necessarily broad and will illuminate the many dimensions of PAEs' conduct in a way that no other entity is capable. Only through the careful study of PAEs conduct can appropriate future policy positions be taken to remedy the harm. At the same time, given the established harm to our economy from frivolous patent assertion, completion of this FTC study should not stay or halt other actions by the administrative, legislative or judicial branches to address this serious issue.

Respectfully submitted,

Michael D. Petricone
Senior Vice President
Government Affairs

December 16, 2013

¹¹ Consumer Electronics Association, Comments of the Consumer Electronics Association to the Federal Trade Commission and Department of Justice Antitrust Division Patent Assertion Entity Activities Workshop (April 5, 2013), available at <http://www.ftc.gov/os/comments/pae/pae-0040.pdf> (visited Dec. 4, 2013).



Consumer Electronics Association
1919 South Eads Street
Arlington, VA
22202 USA
(866) 858-1555 toll free
(703) 907-7600 main
(703) 907-7601 fax
www.CE.org

Federal Trade Commission
Antitrust Division, United States Department of Justice
Patent Assertion Entity Activities Workshop
Comments of the Consumer Electronics Association
April 5, 2013

The Consumer Electronics Association (“CEA”)¹ is pleased to submit these comments on the growing and alarming diversion of resources away from innovation as a result of frivolous lawsuits by so-called Patent Assertion Entities (PAEs or “patent trolls”). As discussed at the December 10, 2012 “Workshop” on Patent Assertion Entities, the harm to our economy that panel members attributed to Non-Practicing Entities (NPEs) is occurring most critically at the smaller firms that have been our most efficient and productive innovators and job creators. The workshop presentations and comments demonstrate that passage of the SHIELD (Saving High Tech Innovators From Egregious Legal Disputes) Act, H.R. 845, is an urgent and necessary step toward reversing this destructive trend.

U.S. patent law exists to promote – not tax or hinder – innovation. The presentations at the Workshop establish, however, that patent law is being misused to damage innovators and entrepreneurs at a rate that hurts innovators and jobs. Litigation and threats of litigation aimed at exploiting imperfections in the patent system are diverting resources and discouraging risk-taking.

Improving the patent review process and the patent system’s overall operation is an important long-term objective – but no presenter forecast that such reform could be sufficiently effective in the immediate future. What *can* be accomplished more urgently is passage of The SHIELD Act, a bill that requires “patent assertion” NPEs (“Patent Assertion Entities,” or “PAEs”) to pay all legal bills if they lose in court because the patent is found to be invalid or there is no infringement. By restoring marketplace balance to decisions about when to litigate patent claims, the SHIELD Act will force PAEs to take financial responsibility for their frivolous lawsuits.

¹ CEA is the principal U.S. trade association of the consumer electronics and information technologies industries, with more than 2,000 member companies. CEA’s International Consumer Electronics Show® (“CES”) is our leading annual showcase for technology innovation.

The problem of frivolous patent litigation brought by PAEs – companies that specialize not in inventing or producing things, but simply in the business of filing patent lawsuits – is growing. Alarming, patent trolls now account for a majority of all patent litigation brought in the United States.²

As the number of lawsuits rises, the penalty paid by innovators grows to enormous proportions. According to a recent Boston University study, in 2009 the aggregate annual direct costs attributed to NPEs was \$13.7 billion. By 2011, it had ballooned to \$29.2 billion.³

The study's more specific conclusions are even more alarming. Specifically, the study found that direct costs of dealing with NPE claims exceed 10 percent of total business spending on research and development. The study also concluded that the burden of defending these frivolous lawsuits falls most heavily on small and medium-sized companies. These companies, our most dynamic job creators, account for 90 percent of entities sued, further they pay a disproportionate share of non-litigated settlements – because they cannot afford the cost of defending against the lawsuit in court, which can frequently be in the millions.

As shocking as these numbers are, they are likely understated, since the study only measured direct costs to businesses from NPE lawsuits, without taking into consideration indirect costs such as diversion of resources, delays in new products, and implications for obtaining investor funding. A 2011 study that measured indirect penalties set overall costs from patent troll litigation at over \$80 billion per year.⁴

At the Workshop, innovators and entrepreneurs testified to the marketplace harms of these run-amok patent lawsuits. The panel presentations by Robin Feldman (Hastings College of the Law), Michael Meurer (Boston University School of Law), Thomas Ewing (Avancept LLC), and Brad Burnham (Union Square Ventures) laid out very clearly how PAEs take advantage of flaws in our patent system while hindering innovation. They noted that the targeting of a company by patent trolls is directly related to the company's success and perceived ability to pay, rather than to any relationship between its products and potential patent infringement. Panelists also detailed the tactic of going after end-users in order to force a settlement. A commonly-used patent troll strategy is to sue large customers of small firms, knowing that the small firm is not in a position to offer indemnification even with respect to very weak claims.

In his presentation, Iain Cockburn (Boston University) summarized the harm to the economy and consumers from these frivolous lawsuits. Litigation-generation misallocations of resources in product investment skew pricing decisions, raising prices for consumers and degrading market efficiency. Meanwhile, the time and focus

² Colleen V. Chien, "Startups and Patent Trolls," Santa Clara University Legal Studies Research Paper No. 09-12, September 28 2012.

³ James Bessen and Michael Meurer, "The Direct Costs from NPE Disputes," Boston University School of Law Working Paper No. 12-34, June 25 2012.

⁴ James Bessen, Jennifer Ford, Michael Meurer, "The Private and Social Costs of Patent Trolls," Boston University School of Law Working Paper 11-45, September 19 2011.

of the victim company's most valuable personnel are diverted to collecting unnecessary information instead of the more productive endeavors for which they were hired. Prof. Cockburn also notes how venture capitalists are frightened away from the riskiest and most potentially successful products because of threat of a lawsuit.

In reality, the results of the Workshop merely confirmed facts that were already well known in the marketplace. Gary Shapiro, CEA's President and CEO, summarized the impact of patent trolls in a *Forbes* article last year:

The patent laws are so unclear that a manufacturer never knows with total certainty whether he is inadvertently violating a patent. Even a successful defense of a patent lawsuit costs upwards of a million dollars, so cash settlements to avoid the nuisance factor are significant. Meanwhile, these lawsuits increase consumer costs for useful products and stifle the creation of any new innovation or product. How did it become a good thing for businesses to be created simply to file lawsuits?⁵

President Obama has shown a keen understanding of the issue. In a recent Google Hangout, he responded to a question about patent trolls by noting:

The folks you're talking about...don't actually produce anything themselves. They're just essentially trying to leverage and hijack somebody else's idea and see if they can extort some money out of them.

While there is no single remedy to the patent troll lawsuit explosion, Congressional passage of the SHIELD Act is a sensible place to start. According to the sponsors of The SHIELD Act:

The proposed SHIELD Act forces patent trolls to take financial responsibility for frivolous lawsuits. If a troll brings a patent lawsuit and loses, the SHIELD Act makes sure that the troll pays all costs and attorney's fees associated with the case. This increased risk will help to deter many trolls from bringing frivolous lawsuits in the first place.⁶

The December 10 panelists demonstrated that the informational and resource allocation harms of PAE litigation and threats were attributable in large part to marketplace and litigation asymmetries. Specifically, PAEs find it efficient to aggregate, threaten, and sue on masses of patents, without any potential responsibility for the defense costs that they engender.

⁵ Gary Shapiro, *Legal Slime Chokes Best Companies*, *Forbes*, August 1 2012, <http://www.forbes.com/sites/garyshapiro/2012/08/01/legal-slime-chokes-best-companies/>.

⁶ Press Release, Chaffetz, DeFazio Introduce Expanded SHIELD Act to Combat Patent Trolls, <http://chaffetz.house.gov/press-release/chaffetz-defazio-introduce-expanded-shield-act-combat-patent-trolls>.

The SHIELD Act addresses these distortions by raising the possibility that an unsuccessful PAE plaintiff may have to pay some of the resource allocation taxes that it seeks to impose. The prospect of cost-shifting should also allow smaller companies that are currently pressured into paying for invalid or non-infringed patents to mount defenses and for their venture investors and customers to stand by them when they do. In short, The SHIELD Act will move the market dynamics around PAE patent litigation and discourage frivolous and opportunistic claims.

The restoration of market dynamics encouraged by the SHIELD Act should also have a beneficial effect on the systemic flaws (as also discussed by panelists) that PAEs exacerbate and abuse. As panelists noted, the absence of adequate information about patents and claims is exploited and amplified by PAEs to produce the most egregious cases. Unless PAEs face at least some of the risks borne by practicing entities in collecting patents and threatening suit, their incentive, and the incentive of those who deal with them, will be to further cloud the information for all concerned, such as examiners, patent seekers, sellers, and aggregators, and potential inventors. Introducing potential litigation costs of the sort faced by other market participants should roll back PAE behavior to better approximate that of market risk-takers. In turn, this should increase, at every level, the incentives to seek and provide accurate information. In time, this pressure may contribute to better functioning of the system itself.

In addition to passage of the SHIELD Act, panelists acknowledged the need for reform of the patent process itself. In a recent article, Jon Potter suggested two core reforms to fix the information defects that PAEs regularly exploit:

First, the Patent Office should require software patent applications to be written in plain language, so they can be easily understood by coders and reasonably smart people. The public has the right to know precisely what is patented, so they know clearly what will be infringing. Patent examiners should be trained to reject applications that do not clearly describe the invention and precisely set out the limits of patent claims.

Additionally, the patent application must describe the invention with enough detail that a reader could actually make and use it. Without sufficient detail, neither an examiner nor the public can be sure that there is really an invention being patented, or whether it is only a non-patentable idea.

We don't patent ideas because that would leave no opportunity for next-generation innovators.⁷

⁷ Jon Potter, San Jose Mercury News, February 11 2013, *Jon Potter: Software patent trolls can be stopped by U.S. Patent Office and Congress*, http://www.mercurynews.com/opinion/ci_22565075/jon-potter-software-patent-trolls-can-be-stopped?fb_action_ids=10151411193764909&fb_action_types=og.recommends&fb_source=other_multiline&action_object_map={%2210151411193764909%22%3A309732665796920}&action_type_map={%2210151411193764909%22%3A%22og.recommends%22}&action_ref_map

If America is to continue to be an economic leader, we must protect innovators, and discourage those who exploit our patent system while creating nothing of value. We recognize that addressing patent abuse is a complex issue and offer our assistance in working with the FTC/DOJ on crafting appropriate and balanced solutions. Further, we believe Congress must move expeditiously to pass The SHIELD Act, the courts should insist that only truly novel and useful ideas receive protection, and the Patent and Trademark Office should strive for accurate and searchable information and definitions in its application process. The Joint Workshop brought attention and scholarship to this vital subject, and provides a well-considered basis for necessary action.

Respectfully submitted,

Michael E. Petricone
Senior Vice President
Government Affairs

April 5, 2013