Before the
DEPARTMENT OF COMMERCE
National Telecommunications and Information Administration

In the Matter of	)	
	)	
The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things	)	Docket No. 160331306-6306-01
	)	
	)	
	)	

COMMENTS OF THE U.S. CHAMBER OF COMMERCE CENTER FOR ADVANCED TECHNOLOGY AND INNOVATION

Amanda Eversole
President

Tim Day
Vice President
U.S. CHAMBER OF COMMERCE
CENTER FOR ADVANCED TECHNOLOGY AND INNOVATION

Megan Brown
Umair Javed
WILEY REIN LLP
Counsel to the Center for Advanced Technology and Innovation

June 2, 2016

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY 2

II. THE "INTERNET OF THINGS" HOLDS INCREDIBLE PROMISE FOR OUR ECONOMY AND QUALITY OF LIFE 4

III. REGULATION OR LEGISLATION WOULD BE PREMATURE GIVEN THE EARLY AND RAPIDLY EVOLVING NATURE OF IOT TECHNOLOGY 7

IV. PRIVATE SECTOR IOT INNOVATION DEPENDS ON INFRASTRUCTURE, VOLUNTARY STANDARDS, AND TECHNICAL NEUTRALITY 8

A. Infrastructure Investment Will Be Critical to the Future of IoT 8

B. The Government Should Make Additional Licensed and Unlicensed Spectrum Available to Support and Promote the Growth of IoT 9

C. Technical Standards for IoT Should Remain Open and Voluntary 10

D. Privacy Concerns Can Be Addressed Under Existing Constructs 11

E. Cybersecurity Will Be Handled through Risk Mitigation, Voluntary Standards, and Information Sharing. 13

V. A NATIONAL STRATEGY SHOULD PROMOTE INVESTMENT, REDUCE REGULATION, AND CHAMPION MARKET-BASED SOLUTIONS GLOBALLY 15

A. Overlapping Federal Approaches Introduce Regulatory Uncertainty and Duplicate Efforts 16

B. NTIA Should Promote a Skilled Workforce for the Digital Future 17

C. NTIA Should Champion Innovation, Openness, and Technology Neutrality Internationally 17

VI. CONCLUSION 20

Before the
DEPARTMENT OF COMMERCE
National Telecommunications and Information Administration

In the Matter of	)	
	)	
The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things	)	Docket No. 160331306-6306-01
	)	
	)	
	)	

COMMENTS OF THE U.S. CHAMBER OF COMMERCE
CENTER FOR ADVANCED TECHNOLOGY AND INNOVATION

The U.S. Chamber of Commerce ("Chamber") Center for Advanced Technology and Innovation ("CATI") welcomes the opportunity to provide input to the Department of Commerce in response to the National Telecommunications and Information Administration's ("NTIA") Request for Comments ("Request") on the current technological and policy landscape for the Internet of Things ("IoT").[1] The Request raises important, cross-sector IoT issues relating to innovation, security, privacy, and international harmonization. These issues require careful thought and NTIA's "holistic economic perspective."[2] A green paper or report from NTIA is a good opportunity to identify emerging issues and focus the federal government on productive activities that support IoT. The Chamber identifies below efforts through which federal agencies—collectively and individually—can expand IoT opportunities while appropriately addressing challenges.

---

1 National Telecommunications and Information Administration, *Request for Comments on the Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things*, 81 Fed. Reg. 19956, 11956 (Apr. 6, 2016) ("Request").

2 *Id.* at 7.

I. EXECUTIVE SUMMARY

The Chamber recently created the CATI to promote the role of technology in our economy and to advocate for rational policies that drive economic growth, spur innovation, and create jobs. As the nation's voice for small and large businesses, the Chamber understands the transformative opportunities IoT presents for consumers, businesses, and our country's economy. The Chamber also appreciates that regulatory and other barriers can impede the development of a nascent IoT and delay the full realization of its many benefits.

IoT represents the next evolution of the Internet and mobility. Much like the Internet's earlier phases, IoT will flourish under a flexible, non-regulatory policy regime. Indeed, for nearly all of the Internet's existence, neither Congress nor regulators rushed to impose regulations on this transformative, disruptive technology. Instead, the U.S. government followed a "hands-off" approach to regulation, allowing the Internet to evolve in response to the market and technical innovation. Similarly, light regulation and uniform federal policy fostered the explosion of wireless connectivity. Today's mobile Internet ecosystem is a driver of innovation, economic growth, and improved consumer welfare. This transformative growth has occurred largely because of the United States' measured approach to regulation.

The lesson for IoT is clear: farsighted regulatory policies that relieve regulatory barriers have a positive effect on the growth of technologies and services. The winners in this process equally are clear: consumers, who not only benefit from enhanced and expanded services, but also from the economic growth and increased opportunities that flow from them.

Given the unqualified success of this approach, NTIA's focus should be on ensuring a similar enabling environment for IoT. The U.S. government should ensure innovators have the freedom to develop solutions that will drive widespread adoption. While NTIA appropriately notes that legal and regulatory challenges may be associated with aspects of IoT, this was also

true of Internet and mobile connectivity. IoT concerns are nascent and in any event, industry—working collaboratively with government in an environment of trust—is best positioned to develop solutions.

As developed below, several steps will help policymakers promote IoT while appropriately addressing challenges and ensuring broader goals. The Administration should:

- **Work to pass the Developing Innovation and Growing the Internet of Things ("DIGIT") Act**. The DIGIT Act will bring together stakeholders in government and industry to shape IoT policy, ensuring that the United States realizes the full economic potential of IoT and remains a leader in this next chapter of the Internet.

- **Reduce regulatory burdens, compliance costs, and overlap**. A multitude of uncoordinated state and federal efforts in IoT is creating an uncertain regulatory environment. Government should evaluate existing regulatory activities and ensure that they are supportive of IoT and do not constitute unintentional barriers.

- **Remove barriers to investment and infrastructure deployment at all levels**. Infrastructure will be critical for IoT deployment, and the government should look for ways to promote deployment and upgrades of communications networks.

- **Champion voluntary, industry-led, globally recognized, and consensus-based processes for technical and interoperability standards**. Historically, the most effective process for developing standards has been driven by the private sector through a variety of open participation, globally recognized, voluntary, and consensus-based standards groups, industry consortia, and companies.

- **Encourage industry and government collaboration to solve evolving security and privacy challenges**. Prescriptive regulation is unnecessary and unwise at this early stage. Approaches to security and privacy must remain collaborative, flexible, and innovative over the long term—enabling solutions to evolve at the pace of the market.

- **Ensure adequate flexible spectrum is available to support IoT**. Ubiquitous high-speed broadband connections over licensed and unlicensed spectrum are critical to the IoT ecosystem. Efficient management of this scarce resource must be a top priority.

- **Promote a skilled workforce capable of operating in the digital future**. Investment in human capital will determine which countries lead in the IoT.

NTIA has led productive multistakeholder processes relating to emerging technologies. The Chamber urges NTIA to continue to convene industry, experts, and stakeholders to address issues that span IoT. This approach is consistent with the Administration's emphasis on

multistakeholder efforts that produce voluntary, flexible approaches to promote innovation and avoid balkanization.[3] NTIA should promote "regulatory humility"[4] to ensure that regulators do not inadvertently hinder IoT development.

II. THE "INTERNET OF THINGS" HOLDS INCREDIBLE PROMISE FOR OUR ECONOMY AND QUALITY OF LIFE

The IoT is empowering people to interact with technology and improve their lives—not only as an evolving technology, but also as a catalyst for innovation. At its core, IoT encompasses unprecedented connectivity. Commissioner Ohlhausen of the Federal Trade Commission ("FTC") aptly described IoT as "[t]he next phase of Internet development [that] is focusing on connecting devices and other objects to the Internet, without the active role of a live person, so that they can collect and communicate information on their own and, in many instances, take action based on the information they send and receive."[5] While it is an evolving concept, IoT includes a myriad of objects—including tags, sensors, and devices—that interact with each other through hardware and software applications to extract meaningful information.

Without question, IoT has revolutionary potential. The IoT "is the next wave of technology, connecting some 50 billion devices, with the potential to unleash significant

---

[3] *See*, *e.g.*, The White House, Report, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy, at 2 (Feb. 2012) (lauding multistakeholder processes and voluntary codes of conduct because "flexibility will help promote innovation" and "effective privacy protections by allowing companies… to address the privacy issues that are likely to be most important to their consumers and users, rather than requiring companies to adhere to a single, rigid set of requirements."); Department of Commerce, Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework (Dec. 2010) (government can "coordinate this process, not necessarily by acting as a regulator, but rather as a convener of the many stakeholders").

[4] "Promoting an Internet of Inclusion: More Things AND More People," Remarks of Commissioner Maureen K. Ohlhausen, Consumer Electronics Show, Las Vegas, NV, at 2 (Jan. 8, 2014), ("Ohlhausen 2014 Remarks"), http://www.ftc.gov/sites/default/files/documents/public_statements/promoting-internet-inclusion-more-things-morepeople/140107ces-iot.pdf.

[5] "The Internet of Things and The FTC: Does Innovation Require Intervention?," Remarks of Commissioner Maureen K. Ohlhausen, U.S. Chamber of Commerce (Oct. 18, 2013), https://www.ftc.gov/sites/default/files/documents/public_statements/internet-things-ftc-does-innovation-require-intervention/131008internetthingsremarks.pdf.

economic growth across the country and the world."[6] According to an oft-cited report, there will be more than 50 billion connected devices by 2020—in just five years, the number of connected objects could grow to over 30 times its size in 2009.[7] Analysts predict that IoT will have a total economic impact in the trillions of dollars. By some accounts, "the IoT has a total potential economic impact of $3.9 trillion to $11 trillion a year by 2025."[8] In the Chamber's view, "[t]he Internet of Things could add as much as $15 trillion to global GDP over the next twenty years."[9]

The benefits of increased connectivity will come from two main areas: consumer-facing IoT and industrial or enterprise IoT. While consumer-facing IoT is what most people think of first, the industrial IoT is expected to account for the lion's share of GDP growth. It is important that policymakers not conflate consumer-facing and industrial IoT.

As the Chamber recognizes, "[t]he Internet of Things will lead to smarter homes, smarter cities, enhanced healthcare, and improved efficiency and productivity."[10] Consumer IoT promises life-changing innovations. Smart homes and home monitoring will promote efficiency, security, and even aging-in-place. Personal wearable and medical devices will improve care and lead to innovations in insurance. Connected and autonomous transportation will improve urban

---

[6] Amanda Eversole, U.S. Chamber of Commerce, "We've Been Talking About the Internet of Things All Wrong," (Mar. 2, 2016), https://www.uschamber.com/above-the-fold/we-ve-been-talking-about-the-internet-things-all-wrong.

[7] Dave Evans, Cisco, The Internet of Things: How the Next Evolution of the Internet is Changing Everything, at 3 (April 2011).

[8] McKinsey Global Institute, Report, Unlocking the Potential of the Internet of Things, at 2 (Jun. 2015), http://www.mckinsey.com/business-functions/business-technology/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world.

[9] Letter from William L. Kovacs, U.S. Chamber of Commerce, to Donald S. Clark, Federal Trade Commission, Project No. P135405, at 2 (dated Jan. 10, 2014), https://www.uschamber.com/sites/default/files/documents/files/1.10.14-%20Comments%20on%20the%20Internet%20of%20Things.pdf ("Chamber IoT Letter").

[10] *Id*.

planning and automotive safety. Even media platforms will be affected, as smart TVs and Virtual Reality impact how consumers experience the world.

Industrial IoT offers equally important innovations, with enormous potential across the global marketplace in agriculture, manufacturing, transportation, and utilities, to name a few. Industrial IoT can protect employees, increase productivity, manage inventory, improve transportation safety and congestion, conduct predictive maintenance, and spur economic growth and competition. With many potentially disruptive technologies promising higher productivity and greener production, industrial IoT may change the global production of goods and services.

Of course, government also stands to benefit from IoT, which can create efficiencies in public services. By finding new value for citizens, enhancing capabilities, and streamlining processes, IoT may provide a much-needed answer for agencies seeking to meet increasing citizen needs with decreasing budgets. The General Services Administration ("GSA"), for example, is using IoT for building maintenance.[11] Connected apps and devices also have the potential to revolutionize public safety, law enforcement, and military operations.

Much is still unknown about the future of IoT, including industry structures, business models, distribution and supply chains, and uses and flows of data from IoT devices. Ultimately, the benefits of IoT will be limited only by the capacity of innovators and by government decisions to allow barriers to persist or instead to pursue policies that support innovation.

In the meantime, companies of all sizes already are leading the way. Pioneering businesses are collaborating with partners on evolving privacy and security solutions, open, consensus-driven standards, and innovative business models and use cases. Access to capital remains strong, enabling even small firms to bring IoT solutions to market. More than 96

[11] *See* GovLoop, Report, The Internet of Things: Preparing Yourself for a Connected Government, https://www.vion.com/assets/site_18/files/gl_guide_iot_final%20(3).pdf.

percent of Chamber member companies are small businesses, with fewer than 100 employees. CATI understands the challenges facing smaller businesses and encourages the Department of Commerce and NTIA to provide a voice for companies of all sizes in the IoT market.

III. REGULATION OR LEGISLATION WOULD BE PREMATURE GIVEN THE EARLY AND RAPIDLY EVOLVING NATURE OF IoT TECHNOLOGY

The transformative potential of IoT will be realized only in a hospitable regulatory environment. IoT is at a similar stage as the Internet was in the 1990s—emerging commercially, with diversity and experimentation, competing standards, and unclear consumer expectations. The Internet's unbridled success results from a minimal regulatory framework, which has been the foundation for the United States' global Internet leadership for decades.

That historical record should inform any federal approach to IoT. Prescriptive legislation is unnecessary and unwise. Premature or reflexive regulation can have unintended consequences, by mandating specifications that become obsolete, or worse, by inadvertently creating security vulnerabilities. Those well-documented risks increase when the government tries to regulate a technologically evolving field like IoT. Unnecessary restrictions here risk limiting opportunities—and U.S. competitiveness—in the global marketplace.

Governments and policymakers are best served by applying a light touch. The DIGIT Act illustrates how IoT should be addressed: through collaboration between government and the private sector on future development and innovation. The Chamber supports the DIGIT Act, which would create a process for government and industry to develop recommendations for a national IoT strategy. The DIGIT Act "recognizes the economic potential of the IoT and will help position the U.S. as a leader in this next chapter of the Internet."[12]

[12] U.S. Chamber of Commerce, "U.S. Chamber's CATI Commends Internet of Things Working Group, Highlights Economic Benefits of Innovative Technology" (Mar. 1, 2016), https://www.uschamber.com/press-

Regulators should refrain from reflexive regulation at this juncture. Even after a national IoT strategy is developed, they should proceed with caution. IoT technology and use will change rapidly, and should be guided by technological advancements, not regulatory classifications or silos.[13] The U.S. government should exercise regulatory restraint, reduce barriers, and empower innovators to develop products that will drive demand.

IV. PRIVATE SECTOR IoT INNOVATION DEPENDS ON INFRASTRUCTURE, VOLUNTARY STANDARDS, AND TECHNICAL NEUTRALITY

A. Infrastructure Investment Will Be Critical to the Future of IoT

Widespread adoption of IoT in homes, cities, and industries will place demands on communication infrastructures and services. Infrastructure will be critical, and the government should look for ways to promote investment, deployment and upgrades of communications networks, including next-generation cellular ("5G") and Wi-Fi. Lack of infrastructure will hinder IoT.

Federal policy has long sought to promote infrastructure improvements to expand communications networks. Wireless operators alone are expected to invest $35 billion annually in mobile broadband infrastructure.[14] This investment is even more critical in a world of burgeoning demand for data services, including IoT. Wireless broadband availability is not only covering more of the population, infrastructure providers are "laying the rails" inside buildings, underground in metros, on university and corporate campuses, in stadiums, retail outlets, and on airplanes. Infrastructure must be built where people and objects congregate.

---

release/us-chamber-s-cati-commends-internet-things-working-group-highlights-economic-benefits.

[13] Ohlhausen 2014 Remarks, at 1-2 ("It is thus vital that government officials, like myself, approach new technologies with a dose of regulatory humility. We can accomplish this by educating ourselves and others about innovation, understanding its effects on consumers and the marketplace, and identifying benefits and likely harms.").

[14] Alan Pearce, Ph.D., J. Richard Carlson, MBA, Michael Pagano, Ph.D., Report, Wireless Broadband Infrastructure: A Catalyst For GDP And Job Growth 2013–2017 (Sept. 2013).

Congress and the Federal Communications Commission ("FCC"), however, have noted that "unreasonable delays" and limits through zoning and access restrictions at the state and local level have been "obstruct[ing] the provision of wireless services."[15] NTIA, the FCC, and all agencies should reduce regulation and limit federal, state, and local barriers to infrastructure deployment. Infrastructure investment will not only be critical to realizing IoT's full potential, it is capable of rapidly creating jobs and technologies that will maintain the nation's technological, political, and economic position.

B. The Government Should Make Additional Licensed and Unlicensed Spectrum Available to Support and Promote the Growth of IoT

A key building block for IoT is access to spectrum under the right terms and conditions. Ubiquitous, high-speed broadband connections over licensed and unlicensed spectrum are critical. The FCC's expert IoT working group predicts IoT will add significant load to existing services, such as Wi-Fi and 4G mobile networks.[16] With analysts heralding some 50 billion connected devices by 2020, the need for additional spectrum for IoT is clear. Effective management of this increasingly scarce resource must be a top priority.

Spectrum needs for IoT will vary depending on technology, from Wi-Fi, Ethernet, Bluetooth, cellular and other communications technologies. Choice of spectrum for different deployments will depend on many factors, including mobility, coverage, QoS/latency, interference resistance, robustness, cost, power consumption, expected life span, and security

---

[15] *Petition for Declaratory Ruling to Clarify Provisions of Section 332(7)(B)*, Order, 24 FCC Rcd 13994, 14006 (2009); *see also* Spectrum Act provisions promoting colocation of wireless equipment, 47 U.S.C. § 1455, and regulations implementing same, 47 C.F.R. § 1.40001. As the FCC and courts have observed, "'[d]espite the widely acknowledged need for additional wireless infrastructure, the process of deploying these facilities can be expensive, cumbersome, and time-consuming …[and] local and Federal review processes can slow deployment substantially, even in cases that do not present significant concerns.'" *Montgomery County Md. v. FCC*, 811 F.3d 121, 125-26 (2016) (quoting *In re Acceleration of Broadband Deployment by Improving Wireless Facilities Siting Policies*, 29 FCC Rcd. 12865 ¶¶ 9-10 (Oct. 17, 2014), amended by 30 FCC Rcd. 31 (Jan. 5, 2015)).

[16] *See* FCC Technological Advisory Council, Presentation, at 12 (2014), https://transition.fcc.gov/bureaus/oet/tac/tacdocs/meeting61014/TACmeetingslides6-10-14.pdf.

needs. It is clear, however, that the number of devices and the nature of traffic will require far more spectrum than is commercially available today.

Government must work with industry to ensure that innovation within and across industry verticals has adequate, flexible spectrum. NTIA and the FCC must be aggressive in making additional licensed and unlicensed spectrum available. Where appropriate, NTIA and the FCC must be creative with spectrum sharing—while protecting incumbents from interference—so that limited resources are used efficiently. Otherwise, uncertainty regarding spectrum will discourage investment and innovation.

C. Technical Standards for IoT Should Remain Open and Voluntary

Technical standardization can reduce barriers to entry to IoT markets and increase economies of scale. However, standards need to be voluntary and carefully designed so that they do not constrain innovation. Historically, the most effective process for developing technical and interoperability standards has been driven by the private sector through open participation, globally recognized, voluntary, and consensus-based standards organizations, industry consortia, and individual companies working together. Governments and policymakers should encourage open standards and commercially available solutions to accelerate innovation and adoption.

The IoT marketplace currently is aligning around industry verticals that are starting to deploy solutions. Although a fragmented ecosystem with non-interoperable technologies could undermine the efficiencies achieved by large economies of scale, tying industry at this early stage to burdensome, conflicting, or one-size-fits-all standards would be harmful. Rapid innovation likely will mean that early approaches quickly will be surpassed. In addition, mandatory standards could tie users to a specific vendor or country requirement to the exclusion of others, which may drive up costs and create barriers to innovation.

Voluntary, industry-led, globally recognized standards can drive secure, flexible, and interoperable solutions that scale across a global IoT ecosystem. Recent standardization efforts for cybersecurity provide a useful example. Like IoT, efforts to improve cybersecurity must reflect the borderless and interconnected nature of our digital environment. Cybersecurity efforts are optimal when they reflect globally recognized standards and industry-driven practices. Cybersecurity standards, guidance, and best practices typically are led by the private sector and adopted on a voluntary basis; they are most effective when developed and recognized globally.[17]

Ultimately, technological maturity and user choice will identify optimal standardization. Whether the topic is interoperability, IP address assignments, cybersecurity, or other technical questions, government should encourage industry collaboration in open participation, globally recognized, consensus-based, and voluntary standards efforts. Government also should champion appropriate standards efforts internationally. This is consistent with federal law promoting commercially driven solutions and reflects the need for standards to mature long before even being considered for incorporation into federal regulatory obligations.[18]

D. Privacy Concerns Can Be Addressed Under Existing Constructs

Without evidence of heightened privacy concerns or consumer harm, there is no reason not to allow the IoT market mature under the frameworks that exist for protecting consumers' legitimate privacy interests. In its recent Staff Report on IoT, the FTC concluded that there was not yet a need to regulate consumer-facing IoT privacy.[19] The Chamber agrees. As with other

---

[17] Letter from Ann M. Beauchesne, U.S. Chamber of Commerce to Michael Hogan and Elaine Newton, National Institute of Standards and Technology (NIST) re: Draft Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity (Sept. 24, 2015).

[18] *See, e.g.*, Office of Management and Budget, OMB Circular A-119, https://www.whitehouse.gov/sites/default/files/omb/inforeg/revised_circular_a-119_as_of_1_22.pdf; *see also* National Technology Transfer and Advancement Act, Public Law 104-113 (1996).

[19] Federal Trade Commission, Staff Report, Internet of Things: Privacy & Security in a Connected World

technologies, the onus is on industry to safeguard consumers and their data, and to communicate appropriate information, consistent with existing privacy regimes. Any consideration of consumer-based IoT privacy should be part of a bigger discussion, which can examine the immense benefits from new uses, as well as best practices, disclosure, and self-regulation.[20]

Prescriptive regulation entails significant costs. We are in the early stages of IoT, and it is not yet clear what heightened privacy concerns IoT poses, if any. Indeed, the privacy issues raised by IoT may be similar to those raised by existing technologies, such as cloud computing; existing approaches are evolving at the pace of the market to safeguard legitimate privacy interests. Moreover, the FTC has not been shy about monitoring consumer-facing IoT and pursuing fraud, misrepresentation, and allegedly unreasonable practices, as it does with other consumer-facing technologies and products.[21]

The FTC and others must resist a temptation to pursue prescriptive solutions to hypothetical problems.[22] For example, in its Staff Report, the FTC suggested practices for data minimization. Because such reports inadvertently can become the basis for enforcement or regulation as they filter through government, government should not follow a "precautionary principle" that might prematurely elevate concerns and chill innovation.

(Jan. 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[20] For example, the automotive industry has voluntarily developed and adopted best practices and guidelines to protect consumer privacy. These principles are based on the Fair Information Practice Principles. See Privacy Principles for Vehicle Technologies and Services (Nov. 13, 2014), http://www.globalautomakers.org/media/papers-and-reports/privacy-principles-for-vehicle-technologies-and-services.

[21] *See, e.g.*, TRENDNet, Inc., (Feb. 2014) (the FTC's "first action against a marketer of an everyday product with interconnectivity to the Internet and other mobile devices– commonly referred to as the 'Internet of Things.'")

[21] Michael Hendrix, "With the Internet of Things, What's to Fear?" (Jan. 29, 2015), https://www.uschamberfoundation.org/blog/post/internet-things-whats-fear/42532.

[22] Registered Perspective on Copyright Review, H. Comm. on the Judiciary (Apr. 29, 2015) (Statement of the U.S. Chamber of Commerce).

To ensure that any future consumer privacy efforts are properly focused, the Chamber suggests that agencies await the DIGIT Act or a similar public and private sector collaboration on a national IoT strategy. Once a national IoT plan is published and IoT use cases are developed, NTIA can oversee a thorough analysis, with private sector collaboration, to determine if there are any gaps or barriers in existing privacy rules and best practices.

NTIA also should call for enterprise or industrial IoT to be carved out of any FTC effort on privacy. The FTC Staff Report acknowledges that the FTC's interest is limited to consumer IoT devices.[23] And, whatever privacy efforts are taken, non-personally identifiable data should continue to be excluded, to continue to encourage appropriate data anonymization.

E. Cybersecurity Will Be Handled through Risk Mitigation, Voluntary Standards, and Information Sharing.

Security is a foundational element, and IoT stakeholders are proactively responding to evolving threats. The wireless sector uses a multilayered, risk-based approach that draws from the entire ecosystem—carriers, OEMs, hardware manufacturers, OS developers, app developers and stores, and users—to address security risks. Industry is tackling security across verticals, including cars, medical devices, wearables, and home products. Public-private partnerships are looking at issues, and industry-focused Information Sharing and Analysis Centers ("ISACs") and Information Sharing and Analysis Organizations ("ISAOs") are sharing information.[24] Third party global standards bodies also are actively engaged. There is no one-size-fits-all approach, and regulation is not the solution. Cybersecurity risks are constantly evolving, so pre-defined, solutions quickly become obsolete. Worse, they could provide bad actors a roadmap for attack.

---

[23] FTC Staff Report at i.

[24] *See, e.g.*, Automotive ISAC; National Health ISAC; Financial Services ISAC; Comm-ISAC.

The best way to address cybersecurity in IoT is through voluntary risk management,[25] investment,[26] and information sharing. Collaboration is critical, and was appropriately promoted in long-sought legislation on cybersecurity information sharing that became law in 2015. The government should examine how to facilitate additional cooperation.

IoT use cases will have different vulnerabilities and risk mitigation, which is why it is important to consider IoT security in the context of a larger discussion. Stakeholders may consider encryption of communications and data, where appropriate. However, encryption will not be appropriate for every sector or use case and is not suitable for a mandate. Stakeholders also may need to balance intellectual property issues as part of their security strategy. Security researchers call for broader copyright circumvention freedom, but "[t]he basic protection against the hacking of copyrighted works has long been understood to be a fundamental aspect of promoting licensed, lawful access to works online."[27] As a foundational matter, the government should not "undermine the protection of section 1201 of the [Digital Millennium Copyright Act]."[28] Finally, stakeholder may face questions about vulnerability disclosures. NTIA has a multistakeholder process for this purpose and notes that "[b]est practices for vulnerability disclosure do exist."[29] Any next steps must promote appropriate research, protect intellectual property, and encourage responsible vulnerability disclosures by avoiding unnecessary customer alarm or regulatory overreaction.

---

[25] *See*, *e.g.*, National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity (Feb. 12, 2014) ("NIST Cybersecurity Framework").

[26] Gartner predicts that worldwide spending on IoT security alone will reach $547 million in 2018. Garnter, Press Release, "Gartner says Worldwide IoT Security Spending to Reach $348 Million in 2016" (Apr. 25, 2016).

[27] Registered Perspective on Copyright Review, H. Comm. on the Judiciary, at 6 (Apr. 29, 2015) (Statement of the U.S. Chamber of Commerce).

[28] *Id*.

[29] NTIA, "Multistakeholder Process: Cybersecurity Vulnerabilities" (Apr. 8, 2016), https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities.

When it comes to cybersecurity, the Chamber has been promoting the National Institute of Standards and Technology ("NIST") Framework for Improving Critical Infrastructure Cybersecurity ("Framework") since it was released in 2014.[30] Chamber members contributed to and are using the framework to manage cybersecurity risks to information networks and systems. Industry is working with government to strengthen information networks and systems. The Framework is effective and cost-efficient for many private-sector organizations because NIST identifies a flexible suite of standards, guidance, and best practices, but avoids presuming to tell companies how to use them.

Security for IoT must remain collaborative, flexible, and innovative—enabling solutions to evolve with the market. These non-regulatory, cooperative, and efficient qualities have drawn industries to the NIST Framework, which is applicable regardless of where a business' operations are situated internationally, and can enhance the cybersecurity of the IoT ecosystem.[31]

V. A NATIONAL STRATEGY SHOULD PROMOTE INVESTMENT, REDUCE REGULATION, AND CHAMPION MARKET-BASED SOLUTIONS GLOBALLY

NTIA should consider how to streamline regulation and remove barriers at the federal, state, and local levels. As NTIA has noted, a "patchwork of regulation threatens to increase costs and delay the launch of new products and services. That, in turn, could dampen investment."[32] Economies of scale mean that larger markets will be important to innovation and connectedness. NTIA should champion an enabling environment domestically and globally.

---

30 *See* NIST Cybersecurity Framework.

31 U.S. Chamber letter to NIST regarding views on the Framework for Improving Critical Infrastructure Cybersecurity, http://csrc.nist.gov/cyberframework/rfi_comments_02_09_16.html (Feb. 9, 2016); U.S. Chamber letter to the European Commission's (EC's) related to the commission's request for stakeholders' views on cybersecurity public-private partnerships (Mar. 11, 2016), https://www.uschamber.com/comment/industry-comment-letter-european-commission-future-cyber-public-private-partnerships.

32 Alan Davidson and Linda Kinney, "Fostering Investment and Innovation in Smart Cities and the Internet of Things (IoT)," NTIA, (Feb. 25, 2016), https://www.ntia.doc.gov/blog/2016/fostering-investment-and-innovation-

A. Overlapping Federal Approaches Introduce Regulatory Uncertainty and Duplicate Efforts

A multitude of uncoordinated state and federal efforts in IoT is creating an uncertain regulatory environment. Multiple federal agencies may have jurisdiction over aspects of IoT, including overlapping rule-making and enforcement authority. State governments and agencies also are active in IoT, resulting in a confusing patchwork of regulations that can interfere with product development and consumer expectations. Many federal and state activities have not kept pace with technological developments. NTIA should seek to simplify the regulatory process and curtail multiple regulatory frameworks that serve as barriers to IoT.

To illustrate, whereas a company making a device for a car previously may have worked with a single government agency, a company developing connected devices for cars today could very well be subject to overlapping or inconsistent federal oversight from a consumer protection regulator (the FTC), a transportation safety regulator (NHTSA), and a spectrum regulator (FCC), among others. A company making medical IoT devices might be subject to FDA, FTC and FCC oversight, and a UAS company might be subject to FAA, FTC, and FCC jurisdiction. In this environment, inter-agency coordination is a must to avoid stifling innovation, slowing GDP growth, reducing predictability, and multiplying burdens.

State and local interests also can impede rapid, scaled deployment. Vague state laws, such as those about gathering consumer data, can stifle innovation. Technical mandates, like those mandating a smartphone "kill switch" or encryption, can balkanize markets, interfere with product development and distort consumer expectations. Finally, barriers to infrastructure deployment from zoning and land use limitations can slow the building and upgrading of

---

smart-cities-and-internet-things-iot.

wireless facilities that will be essential to IoT. The federal government should look for those barriers and seek to eliminate them.

A national strategy for IoT, such as one developed under the DIGIT Act, can forestall problems by sending a clear message that over-regulation or poorly-designed regulation threatens IoT growth. A national strategy can encourage regulators to focus on activities that would expand, rather than limit, the use of the IoT. This is critical for U.S. competitiveness, particularly as other countries adopt policies to encourage IoT innovation within their borders.[33]

B. NTIA Should Promote a Skilled Workforce for the Digital Future

Educational systems in most countries, including the United States, are not keeping pace with the demands of a rapidly changing digital world. IoT will place a new premium on skills, innovation, and adaptability, and policymakers must understand how to adapt the education system to better align with technological advancements. Indeed, investment in human capital development will be a critical determinant of which nations lead in the IoT. The United States must continue to foster and educate a technologically savvy workforce, through investments in education and other policies that promote a skilled workforce.

C. NTIA Should Champion Innovation, Openness, and Technology Neutrality Internationally

Many countries are promoting IoT—establishing national blueprints with time-bound goals, investing in research and deployment, and launching public-private partnerships. At the same time, regional and intergovernmental organizations are staking out early roles on IoT policy and technology. Economies of scale mean that these international activities may impact

[33] For example, Germany is working to remove barriers to testing autonomous vehicles on public roads, and the U.K. plans to test on public roads in 2017 and permit full operation in 2020. Michael Nienaber, "Germany Keen to Test Self-Driving Cars on the Road," Reuters, (Apr. 12, 2016), http://www.reuters.com/article/us-germany-autos-merkel-idUSKCN0X915A; "Costas Pitas, Britain to Test Driverless Cars on Motorways from Next Year," Reuters, (Mar. 12, 2016), http://uk.reuters.com/article/uk-britain-autos-driverless-idUKKCN0WE0HX.

IoT deployment and adoption. NTIA should support U.S. IoT innovation by ensuring that the U.S. stays ahead and globally champions policies that support IoT, such as open, consensus-based, and globally recognized standardization efforts, open markets, the seamless flow of information, and technology neutrality.

Countries like China, Korea, India, Germany, Brazil, and other are moving ahead on IoT. In May 2014, for example, the Korean government published its plan for building the IoT with the aim of a hyper-connected, "digital revolution".[34] It targets the commercialization of 5G mobile communications by 2020 and aims for Gigabit Internet to achieve 90 percent national coverage by 2017. Some countries, like China and India, are providing financial incentives or subsidies for IoT. India's Smart City plan is part of a larger agenda of creating Industrial Corridors between India's big metropolitan cities and seeks to create seven new smart cities. Brazil, in turn, is encouraging IoT with favorable tax policies and Germany has launched innovation clusters tied to IoT.

Regional and intergovernmental bodies also are seeking to gain influence. The United Nation's International Telecommunication Union ("ITU") has created a study group focused on standardizing end-to-end architectures and interoperability of IoT. The work of this group duplicates—and may conflict with—other global industry efforts. Moreover, in contrast to other open-participation standardization efforts, the ITU is more bureaucratic and slow-moving, with control exercised by ITU Member countries in a one-country, one-vote system.

IoT has been an important part of the European Union's "Digital Agenda." The EU created the Alliance for Internet of Things Innovation and suggested regulations on privacy, security, consumer protection, and competition. The Body of European Regulators ("BEREC")

[34] Ministry of Science, ICT, and Future Planning, Master Plan for Building the Internet of Things that Leads the Hyper-Connected, Digital Revolution (Aug. 2014).

assessed whether M2M services might require special treatment. Some EU efforts may conflict with work in multistakeholder groups and raise barriers for non-EU companies.

The U.S. government must remain vigilant, and guard against global efforts that might endanger the open, consensus-based, private sector-led system of standards development that fosters innovation. NTIA recognizes the importance of such a policy in the recently updated Circular A-119.[35] The U.S. government also should remain vigilant against data privacy measures that distort competition. Forced localization, including requirements to use local servers and infrastructure to store data, is an immediate threat to the growth IoT growth. NTIA and the U.S. government must step up efforts to avoid measures that require data localization, including advocating for strong, enforceable rules in trade agreements and countering unequal treatment for companies headquartered in the United States.

[35] *See, supra*, n.18.

VI. CONCLUSION

The Chamber strongly supports the Department of Commerce's efforts to encourage growth of the digital economy and ensure that the Internet remains an open platform for innovation. There are several ways that the U.S. government can facilitate and remove impediments to the development of IoT. Only a market driven, industry-led approach will unleash the full potential in the IoT space.

Respectfully submitted,

/s/ Amanda Eversole
Amanda Eversole
President

Tim Day
Vice President
U.S. CHAMBER OF COMMERCE
CENTER FOR ADVANCED TECHNOLOGY AND INNOVATION

Megan Brown
Umair Javed
WILEY REIN LLP
Counsel to the Center for Advanced Technology and Innovation

June 2, 2016