Statement of the Chamber Technology Engagement Center

ON: HEARING ON "Internet of Things Legislation"

TO: U.S. HOUSE ENERGY AND COMMERCE COMMITTEE, SUBCOMMITTEE ON DIGITAL COMMERCE AND CONSUMER PROTECTION

DATE: May 22, 2018

1615 H Street NW | Washington, DC | 20062

BEFORE THE U.S. HOUSE ENERGY AND COMMERCE COMMITTEE,
SUBCOMMITTEE ON DIGITAL COMMERCE AND CONSUMER PROTECTION
Hearing on "Internet of Things Legislation"
Testimony of Tim Day
Senior Vice President, Chamber Technology Engagement Center

May 22, 2018

Good morning, Chairman Latta, Ranking Member Schakowsky, and distinguished members of the House Subcommittee on Digital Commerce and Consumer Protection. My name is Tim Day and I am the Senior Vice President of the Chamber Technology Engagement Center (or C_TEC). C_TEC was created to promote the role of technology in our economy and to advocate for rational policies that drive economic growth, spur innovation, and create jobs. C_TEC understands the transformative opportunities IoT presents for consumers, businesses, and our country's economy. C_TEC 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. Light regulation and uniform federal policy fostered the explosion of both wireline and 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, the focus of policymakers 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. 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. *Today's draft study language takes a step in the right direction to alleviate these burdens*.

- **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.

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

I. 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. Former Acting Chairman 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."[1] 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. One study projects the number of IoT devices by 2020 will reach 20.4 billion.[2] 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."[3] In C_TEC's view, "[t]he Internet of Things could add as much as $15 trillion to global GDP over the next twenty years."[4]

---

[1] "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.

[2] Liam Tung, "IoT devices will outnumber the population this year for the first time," ZDNet (Feb. 7, 2017) *available at* https://www.zdnet.com/article/iot-devices-will-outnumber-the-worlds-population-this-year-for-the-first-time/.

[3] 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.

[4] Letter from William L. Kovacs, U.S. Chamber of Commerce, to Donald S. Clark, Federal Trade Commission,

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 do not conflate consumer-facing and industrial IoT.

As C_TEC recognizes, "[t]he Internet of Things will lead to smarter homes, smarter cities, enhanced healthcare, and improved efficiency and productivity."[5] 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 planning and automotive safety in smart cities. Even media platforms will be affected, as smart TVs and Virtual Reality will 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.[6] 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 the 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.

II. 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,

---

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").

[5] *Id.*

[6] *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.

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.

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.[7] The U.S. government should exercise regulatory restraint, reduce barriers, and empower innovators to develop products that will drive demand.

III. 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. According to Accenture, one component of the wireless infrastructure necessary—5G—will lead to $275 billion in investment that will create 3 million new jobs and $500 billion in U.S. GDP growth.[8] 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.

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

[7] 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.").

[8] "Smart Cities: How 5G Help Municipalities Become Vibrant Smart Cities" Accenture (2017) *available at* https://www.accenture.com/t20170222T202102Z__w__/us-en/_acnmedia/PDF-43/Accenture-5G-Municipalities-Become-Smart-Cities.pdf.

level have been "obstruct[ing] the provision of wireless services."[9] FCC Commissioner Brendan Carr's plan to reduce these regulatory barriers and make America 5G ready is also a step in the right direction to deploy connectivity.[10] More can be done and both Congress and 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.[11]

B. 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.[12]

---

[9] *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)).

[10] Tim Day, "Here's How to Make Cities Smarter," *Above the Fold* (Mar. 22, 2018) *available at* https://www.uschamber.com/series/above-the-fold/here-s-how-make-cities-smarter.

[11] Jordan Crenshaw, "Three Ways to Bring Communications Regulations into the Digital Age," *Above the Fold* (Nov. 15, 2017) *available at* https://www.uschamber.com/series/above-the-fold/three-ways-bring-communications-regulations-the-digital-age.

[12] Letter from Ann M. Beauchesne, U.S. Chamber of Commerce to Michael Hogan and Elaine Newton, National

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.[13]

C. Privacy Concerns Should be Addressed in a Technologically Neutral Way

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 2015 Staff Report on IoT, the FTC concluded that there was not yet a need to regulate consumer-facing IoT privacy.[14] C_TEC agrees. As with other 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.[15]

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.[16]

The FTC and others must resist a temptation to pursue prescriptive solutions to hypothetical problems.[17] For example, in its Staff Report, the FTC suggested practices for data minimization. Because such reports inadvertently can become the basis for enforcement or

---

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).

[13] *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).

[14] Federal Trade Commission, Staff Report, Internet of Things: Privacy & Security in a Connected World (Jan. 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[15] 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.

[16] *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.'")

[16] 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.

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

regulation as they filter through government, government should not follow a "precautionary principle" that might prematurely elevate concerns and chill innovation.

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

Congress should consider how to streamline regulation and remove barriers at the federal, state, and local levels. As the National Telecommunications and Information Administration (NTIA) noted, a "patchwork of regulation threatens to increase costs and delay the launch of new products and services. That, in turn, could dampen investment."[18] Economies of scale mean that larger markets will be important to innovation and connectedness. NTIA should champion an enabling environment domestically and globally.

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. Policymakers 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 the FDA, FTC and FCC oversight, and a UAS company might be subject to the 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. Today's legislation at issue is a step in the right direction toward unraveling the web of duplicative regulatory frameworks.

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

[18] 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-smart-cities-and-internet-things-iot.

A national strategy for IoT 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.[19]

B. Policymakers 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. Policymakers 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 IoT deployment and adoption. Policymakers should support American 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 others are moving ahead on IoT. In May 2014, the Korean government published its plan for building the IoT with the aim of a hyper-connected, "digital revolution."[20] 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.

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

[19] 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.

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

Circular A-119.[21] 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 of IoT. 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.

V. CONCLUSION

IoT is already and will continue to impact the daily lives of all Americans. This connected technology is revolutionizing the health, manufacturing, transportation, and agricultural sectors to name a few. IoT is also becoming an economic game-changer which will inject billions of dollars into the U.S. economy. That is why it is so important for the United States to lead international in technology. In order for this to be achieved, Congress and the agencies that oversee IoT should avoid duplicative as well as overly-prescriptive and burdensome regulation that impede innovation. Technology, including IoT, is a force for good that should be fostered by smart regulatory frameworks that encourage investment, promote innovation, as well as connect and empower Americans from all walks of life.

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