Department of Commerce
National Telecommunications and Information Administration
Request for Comments
The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things
Docket No. 160331306

I. Introduction

ITI represents 60 of the nation's leading information and communication technology companies.[1] ITI is the voice of the high-tech community, advocating for policies that advance U.S. leadership in technology, promote innovation, open access to new and emerging markets, protect and enhance consumer choice, and foster increased global competition. Our membership includes companies from all verticals of the technology sector, including semiconductor, network equipment, software, digital services, hardware, mobile device, and Internet companies. As such, ITI has a broad perspective on the transformational economic, societal, and commercial opportunities the Internet of Things (IoT) is creating, and appreciates the opportunity to comment in this proceeding.[2]

II. Defining and Categorizing the IoT

The IoT is a collection of external devices and sensors that generate data, which, through an Internet connection, can be analyzed to provide actionable information. It is estimated that by 2020 approximately 30 billion devices will be connected through the IoT, representing a 20 percent growth when compared to the 10 billion objects connected in 2013.[3] Moreover, by 2025, the IoT is expected to generate $11.1 trillion in economic potential.[4]

The range and application of these devices is virtually limitless, but is generally viewed in three distinct categories: 1) commercial or industrial, 2) personal or mobile, and 3) household.

---

[1] For more information on ITI, including a list of its members, please visit http://www.itic.org/about/member-companies. ITI's member companies have diverse business interests and though is filing generally reflects the views of ITI's membership, any specific company's views may not align in part, or in whole, with a position that is reflective of the broader membership.

[2] Department of Commerce, Request for Comments, The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things, Docket No. 160331306, (hereafter referred to as "RFC").

[3] *The Internet of Things: Sizing Up the Opportunity*, McKinsey & Company, December 2014, http://www.mckinsey.com/industries/high-tech/our-insights/the-internet-of-things-sizing-up-the-opportunity.

[4] *Ibid*.

Commercial or Industrial IoT Technologies
Commercial and industrial IoT devices are by far the largest category, and the area where many of our companies see the biggest opportunity to enhance productivity and efficiencies, improve real-time decision making, and solve critical societal problems. Estimates for this specific category of IoT are predicted to eclipse $7 trillion by 2030.[5] This category includes predictive maintenance of equipment, facility heating, cooling and lighting management, transportation fleet management and improvement, and many other large scale uses where the aggregate of small changes on a large scale equates to significant cost, energy, and other efficiency and productivity improvements. Roughly 70 percent of the potential value from the IoT comes from commercial and industrial IoT applications.[6]

Personal or Mobile IoT Technologies
Personal or mobile IoT technologies – including wearable watches, health monitors, and similar devices that connect to the Internet via wireless broadband or through a mobile phone – are ubiquitous. The defining characteristic of this category is the mobile nature of the IoT application and the reliance on a wireless broadband connection. It is should be underscored that the real gross domestic product (GDP) impact from this category will be derived from intelligent and autonomous vehicles and cars connected to the Internet via cellular or other wireless technologies. Already, intelligent and autonomous vehicles are predicted to generate between $210 billion and $740 billion in economic growth.[7]

Household IoT Technologies
Household IoT applications range from smart appliances to smart thermostats, and intelligent home monitoring and security systems. These products will connect through a residential broadband connection or home Wi-Fi networks to provide energy savings and home automation and security benefits.

III. Economic and Societal Benefits of the IoT

The societal and economic benefits generated from the IoT are endless. Presented below is a set of examples demonstrating the overall potential of the IoT; the list is intended to be illustrative rather than exhaustive.

---

[5] *CEO Briefing 2015, From Productivity to Outcomes: Using the Internet of Things to Drive Future Business Strategies*, Accenture, 2015, https://www.accenture.com/t20150527T211103__w__/fr-fr/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Local/fr-fr/PDF_5/Accenture-CEO-Briefing-2015-Productivity-Outcomes-Internet-Things.pdf.
[6] *The Internet of Things: Sizing Up the Opportunity*, McKinsey & Company.
[7] *Ibid*.

Commercial or Industrial IoT Technologies
IoT technologies are expected to derive significant economic productivity when applied to business-to-business (B2B) applications. For example, the integration of IoT technologies across all standardized production environments (i.e., factories, hospitals, and agricultural settings) will produce between $1.2 trillion and $3.7 trillion in economic opportunities as a result of energy and labor efficiencies.[8] Similarly, IoT technologies are predicted to yield $470 billion and $360 billion per year in savings due to overall operations improvements and equipment maintenance in custom production environments (i.e., mines, oil, and gas extraction sites).[9] Lastly, IoT office applications possess countless energy management and security benefits, and could generate between $70 billion to $150 billion in economic impact when fully materialized.[10]

Personal or Mobile IoT Technologies
IoT technologies within this category offer a number of exciting solutions aimed at helping individuals, as well as physicians, prevent and diagnose a number of health conditions. For example, by regularly collecting data pertaining to their own health (e.g., weight, activity level, and sleep cycles), individuals can more easily recognize potential health issues and seek medical treatment earlier.[11] Studies have indicated preventable health conditions account for 80 percent of overall disease burden and an astounding 90 percent of total health care costs. IoT technologies not only have the potential to increase overall life-quality, but also stand to decrease health care related expenses.

As noted previously, intelligent and autonomous vehicles technologies are also expected to generate significant economic and societal benefits. According to the World Health Organization (WHO), there were 1.24 million deaths on the world's roadways in 2010,[12] while the U.S. Census Bureau reported there were 10.8 million accidents on U.S. roadways in 2009.[13]

---

[8] *The Internet of Things: Mapping the Value Beyond the Hype*, McKinsey & Company, June 2015, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0ahUKEwjpt4Go8YnNAhXGpB4KHWLLCZ4QFggjMAE&url=http%3A%2F%2Fwww.mckinsey.com%2F~%2Fmedia%2FMcKinsey%2FBusiness%2520Functions%2FBusiness%2520Technology%2FOur%2520Insights%2FThe%2520Internet%2520of%2520Things%2520The%2520value%2520of%2520digitizing%2520the%2520physical%2520world%2FUnlocking_the_potential_of_the_Internet_of_Things_Executive_summary.ashx&usg=AFQjCNGkvbjbBhjdQuj3pC_n4kmWr8EE_w&sig2=8lx339S-halSCfYuLrBdqA.
[9] *Ibid*.
[10] *Ibid*.
[11] *The Internet of Things,* Center for Data Innovation, November 2013, http://www2.datainnovation.org/2013-internet-of-things.pdf.
[12] *Global Health Observatory Data: Number of Road Traffic Deaths,* World Health Organization, http://www.who.int/gho/road_safety/mortality/en/.
[13] *Statistical Abstract of the United States: 2012*, U.S. Census Bureau, Section 23: Transportation, 1101, Motor Vehicle Accidents,

It is believed that human error contributes to 90 percent of automobile accidents,[14] and autonomous vehicles can prevent 90[15] percent of all these accidents. Moreover, recent studies have also concluded that the wide adoption of advanced driver assistance systems (ADAS), which are already on the market, could reduce 28 percent of all motor vehicle crashes in the United States, preventing more than 9,900 fatalities annually.[16]

Directly related to this are also the economic benefits derived from the reduction in accidents. The economic cost of automobile accidents stem from property damage, lost earnings, lost household earnings, medical costs, legal costs, and many other impacts. Annual costs from injuries amount to $365 billion, and costs from fatalities account $260 billion. If there were a 90 percent reduction in accidents, the positive economic impact would be more than half a trillion dollars, or $563 billion.[17]

Countless other benefits, both economic and societal, will be derived from autonomous and connected vehicles, including increased productivity from time not spent focusing on driving, decreased congestion, and fuel savings from less congested roadways. These technologies will also increase the mobility of individuals not capable of operating a vehicle today, namely the elderly, disabled, and youth; providing much more convenient, safe, and flexible transportation options that may currently be unavailable to these populations. The economic impacts from this increased safety and reduction of accidents, reduced fuel consumption, and added productivity has been estimated to be more than a trillion dollars.[18]

Household IoT Technologies

There is a broad range of IoT devices and applications increasingly being utilized in homes. These devices include smart appliances and self-guided vacuum cleaners, among others, and are expected to decrease 100 hours of labor annually for a typical household through efficient chore automation. Moreover, these devices and applications can assist households in managing their energy consumption, leading to nearly $110 billion in overall savings.[19] For

---

http://www.census.gov/library/publications/2011/compendia/statab/131ed/transporation.html.

[14] *The Economic Benefits of Driverless Cars*, Morgan Stanley, February 2014, https://robotenomics.com/2014/02/26/morgan-stanley-the-economic-benefits-of-driverless-cars/.

[15] *Urban Mobility at a Tipping Point*, McKinsey and Company, September 2015, http://www.mckinsey.com/insights/sustainability/urban_mobility_at_a_tipping_point.

[16] *A Roadmap to Safer Driving Through Advanced Driver Assistance Systems*, The Boston Consulting Group, 2015, http://www.mema.org/Document-Vault/PDFs/2015/MEMA-BCG-ADAS-Report.pdf.

[17] *Nikola's Revenge: TSLA's New Path of Disruption*, Morgan Stanley Research North America, February 25, 2014, 24-26.

[18] *Ibid.,* 24.

[19] *The Internet of Things: Mapping the Value Beyond the Hype*, McKinsey & Company.

example, families are able to decrease their energy costs by purchasing appliances capable of communicating with the smart grid to optimize energy based on dynamic price signals.[20] Furthermore, connected thermostats are now being advertised as saving homeowners approximately $173 per year by decreasing energy consumption by 20 percent through optimal utilization.[21]

IV. Governments Should Leverage Trade and Investment Agreements to Support the Growth of the IoT

Data is the lifeblood of the global economy. In today's connected world, international commerce simply cannot function without constant streams of data flowing across borders. The free movement of data allows U.S. companies of all sizes and in all industries to bring new innovations to global markets, driving investment, growth, and job creation. Cross-border data flows particularly enable small and medium-sized enterprises (SMEs) to compete in the global economy. Access to digital products and services, such as cloud applications, provides smaller companies with cutting-edge services at competitive prices, enabling them to participate in global supply chains and directly access customers in foreign markets.

Unfortunately, governments around the world are considering or are already imposing digital trade barriers. American companies have the most to lose if these barriers are not addressed. To support the growth of the IoT and the continued competitiveness of the American economy, the U.S. Government (USG) should aggressively protect cross-border data flows through bilateral and plurilateral trade agreements. The Trans-Pacific Partnership (TPP) includes new and innovative disciplines protecting the legitimate flow of data across borders. The Trans-Atlantic Trade and Investment Partnership (TTIP) and the Trade in Services Agreement (TiSA) provide important opportunities to build upon these TPP disciplines and help write the "rules of the road" for future trade agreements. Specifically, these agreements must include binding provisions protecting cross-border data flows and preventing "data localization" through requirements to use local data centers.

It is also important to note that existing trade and investment agreements contain binding commitments that are important for the IoT, including provisions on transparency, predictability, and nondiscrimination in the application of laws and regulations, on trade in goods and services, and on protection of intellectual property. The United States should continue to leverage these commitments to respond to protectionist policies that could undermine existing rights and obligations.

[20] *The Internet of Things,* Center for Data Innovation.
[21] *Ibid*.

V. Existing Authorities, Government Activity, and Industry Leadership

In many ways, the IoT is not new. Since the Internet was invented, various devices have been connected and networked in attempts to improve convenience, functionality, and for many other purposes, and that is still the case today, albeit with much greater success and on a more pervasive scale. In fact, the first "connected toaster" – an example which has seemed to occupy the fascinations of many as a questionable IoT application – dates back to 1990.[22] What is new, however, is the rapid growth of networked devices and Internet applications due to lower computing costs, increased ability to analyze complex data, availability of components, expansive and lower cost Internet service, and the lower cost of technology that makes Internet connection possible.

Given the IoT is just another evolution of technology, existing laws, and industry best practices for the most part already exist that would cover IoT products. There is not a need, nor would it make sense, to create IoT-specific legislation or regulation. Indeed, the IoT would fall under *comprehensive* legislation, regulation, and industry best practices. For example, comprehensive privacy or security legislation and regulation now and in the future would cover the IoT, just as it would other technologies and products. The recognition of IoT falling under comprehensive legislation or regulation, or industry best practices, is key for policymakers who may be eager to legislate or regulate this newest evolution of technology.

As such, the USG and other government bodies, in consultation with industry, first must assess where current authority, oversight, regulation, or voluntary industry best practices already exist – as well as where they already may be in the works. Indeed, government should seek to identify areas where government and industry oversight and best practices exist as part of larger, more comprehensive best practices, legislation or regulation. The following examples are not exhaustive but demonstrate where comprehensive authorities already exist which cover the IoT, where government is facilitating IoT development, and where industry is working with government to address what may be perceived as new or evolving issues.

Privacy

Comprehensive privacy regulation already exists that would cover the IoT. With the exponential growth in the number of devices that will produce, and analyze, or transmit data, questions around data privacy arise. At the outset, it is important to keep in mind that a significant amount of data will have no connection to a person or individual; industrial or commercial IoT applications will largely be used for diagnostic, logistic, or other performance-related purposes, which does not raise the privacy concerns of consumer use cases (personal/mobile, household). Secondly, data that is de-identified or anonymized and aggregated does does not raise the same privacy concerns as other collections and uses of data.

[22] Thomas Newton, *Internet Connected Toasters: A History*, Recombu, April 14, 2012, https://recombu.com/digital/article/internet-connected-toasters-a-history_M10281.html#.

In applications, including IoT use cases, where data that identifies individuals is collected, the collection, use, sharing, and protection of such data are already subject to existing laws. It should be underscored that many of the benefits derived by the IoT will come the use of personal consumer data. Nevertheless, consumer products, including consumer IoT products, fall within the jurisdiction of the Federal Trade Commission (FTC) and are thus subject to its unfair or deceptive acts or practices authority under Section 5 of the Federal Trade Commission Act. Grounded in Fair Information Practices Principles (FIPPs), the FTC's approach to privacy helped enable the Internet to thrive and, as a consequence, ITI companies have been able to offer an expanding range of services and applications (including IoT applications), often times free or at a nominal expense to consumers. While all FIPPs protections may not be applicable in all instances and flexibility may be necessary for certain IoT applications,[23] the FTC, in conjunction with industry best practices, already has the expertise and authority to oversee privacy matters. In fact, the FTC has taken action in this space and brought a settlement against TRENDnet Inc., a company that markets Internet enabled video cameras.[24] In that case, the company failed to implement reasonable security measures, resulting in transmission of live video feeds from consumers' homes on the Internet.

Depending on the IoT use case, data collected, and the actors involved, other comprehensive statutory authorities may also be applicable to IoT products or services. For instance, there are certain protections for health information under the Health Insurance Portability and Accountability (HIPAA) Act and the Health Information Technology for Economic and Clinical Health (HITECH) Act, while the Graham-Leach-Bliley (GLB) Act and the FTC's Safeguards Rule govern the protection of information held by financial institutions.

Security

Significant activity continues to take place across both government agencies and the private sector in an effort to strengthen cybersecurity. The interests of government agencies and industry are aligned in this arena in that both aim to minimize vulnerabilities and create networks, products, and devices that are as secure as possible. Consequently, much of the activity designed to enhance cybersecurity takes place via voluntary consultation and close collaboration with the private sector, and we strongly encourage that approach to continue.

ITI's member companies are at the forefront of providing security solutions from the devices at the expanding network edge to the cloud, and across the network and the IoT. With billions of additional devices coming online, ITI's companies embed security measures in IoT platforms at the outset of the manufacturing and design process for each new device that extends and expands the network. Security built into both hardware and software at the outset provides redundancies, to help prevent intrusions, and to create more secure and trusted IoT systems. For example, semiconductor manufacturers are increasingly designing chips with built-in safeguards. Encryption, for instance, is increasingly occurring at the transistor level, giving chips

[23] *See* In the Matter of the Internet of Things, ITI Comments to FTC, FTC Project No. P135405, January 9, 2014.

[24] *See* In the Matter of TRENDnet Inc., FTC File No. 122 3090, September 11, 2013.

immutable identifiers that prevent them from being rewritten. Similarly, on the network side, devices communicating with the network are being designed to require an increasingly reliable level of service and connectivity, as well as high security to help prevent unwanted intervention. New Internet protocol architectures are more adaptable and use advanced technologies to more pervasively distribute security, treat individual users and devices with an appropriate level of performance and privacy based on their needs, and automate manual processes to improve scale and availability.

Excellent public-private groundwork has already been laid with respect to comprehensive security best practices that should be leveraged going forward for all technologies, including the IoT. The technology sector has been voluntarily partnering with the National Institute of Standards and Technology (NIST) for nearly three years in developing and using the Framework for Improving Critical Infrastructure Cybersecurity (Framework).[25] The Framework stems from Executive Order 13636,[26] issued in February 2013, which called for the government to partner with owners and operators of critical infrastructure to improve cybersecurity through the development and implementation of risk-based standards. Development occurred through a process of coordination and collaboration convened by NIST between the technology industry, others in private industry, and USG partners. What resulted is a set of voluntary guidelines, best practices, and standards to help critical infrastructure, businesses, and other private and public actors to better manage cybersecurity risks. Taking a similar public-private partnership approach, NIST recently released a Draft Framework for Cyber-Physical Systems[27] (CPS Framework) that was developed in partnership with industry, academic, and government experts. One of the key working groups in the cyber-physical systems project is focused on cybersecurity and privacy.[28]

ITI believes it is pivotal to continue to replicate this voluntary public-private partnership approach in addressing IoT cybersecurity and other challenges. The NIST Framework provides an overarching structure, grounded in proven international standards and consensus best practices, to address organizational security across all critical infrastructure sectors, while providing adaptability and flexibility to meet the unique needs of each sector and address new threats. The cyber-physical systems framework will provide additional technical details for building secure products for the IoT. Conversely, viewing cybersecurity uniquely for each application, whether it be a home computer or an automobile, is far too inflexible and will leave US industry less able to quickly and efficiently respond to new threats, potentially stifling innovation around security – and threaten U.S. innovation and global leadership.

---

[25] *See* Framework for Improving Critical Infrastructure Cybersecurity, National Institute of Standards and Technology (NIST), http://www.nist.gov/cyberframework/index.cfm.
[26] *See* Executive Order 13636 Improving Critical Infrastructure Cyber Security, https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurityWhite House, https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.
[27] *See* CPS Draft Framework, NIST, http://www.cpspwg.org.
[28] *See* CPS PWG Cybersecurity, NIST, http://www.nist.gov/cps/cpswpg_security.cfm.

Perhaps of more concern is the potentially counterproductive precedent of creating siloed approaches to cybersecurity across different IT applications, as part of the IoT and beyond. As more aspects of our daily lives increasingly become digitized, and more "things" are indeed connected to the internet in order to make our lives richer and more efficient, we do not need to reinvent the wheel when it comes to security as each of these applications or use cases gains prominence. For example, at different stages of the recent past, policymakers have considered whether new regulatory regimes were needed to better secure critical infrastructure, the electric grid, cloud computing, or health IT, and in each instance, after close examination, the benefits of approaches grounded in voluntary, consensus-based international standards that can both promote innovation and preserve the promise of interoperability have carried the day. The alternative – a world in which we endeavor to separately regulate each new application or IoT use case or vertical – is unsustainable.

Another area in which the government can provide leadership is to make certain that efforts to improve cybersecurity leverage public-private partnerships and build upon existing initiatives and resource commitments. The technology industry, along with our peers in other industry sectors, leads and contributes to a range of significant public-private partnerships, including information sharing, analysis, and emergency response with governments and industry peers. Two key examples of public-private partnerships the government can prioritize to ensure greater coordination and collaboration across the government are information sharing and analysis centers (ISACs), and sector coordinating councils (SCCs).

While ISACs across a number of industry sectors have been in existence for varying periods of time, and thus have different experience levels in responding to threats and vulnerabilities, more mature ISACS, such as the Information Technology ISAC (IT-ISAC) (formed in 2000 and operational in 2001) and the Financial Services ISAC (launched in 1999), have developed best practices for effectively receiving and distilling threat information and working with the groups' members. The ISACs are invaluable in helping address sector specific and cross-sectoral threats and vulnerabilities. For example, the IT-ISAC helped monitor and collaborate with its members on large-scale threats such as Conficker and the DNS Cache Poisoning Vulnerability. The IT-ISAC provided a forum for members to engage in collaborative analysis on those significant issues, and to draft and share analytical alerts with remediation suggestions that were shared with members, partner ISACs, and the public. Mirroring the growth of the IoT, we now see new ISACs being formed, such as the Automotive ISAC (formed approximately a year ago), which can benefit from the experiences of the more established ISACs. Close collaboration between the IT-ISAC and the Automotive ISAC could provide valuable lessons and solutions to new problems based on variations of issues that may have been faced by the technology sector in the past. The same may be true as other sectors that previously did not face vulnerabilities due to technology or software become increasingly connected to the network.

The SCCs are self-organized and self-governed councils enabling critical infrastructure owners and operators, their trade associations, and other industry representatives to interact on a wide range of sector-specific strategies, policies, and activities related to cybersecurity. The SCCs

coordinate and collaborate with their counterparts across the USG, primarily their sector-specific agencies and related Government Coordinating Councils (GCCs), to address and facilitate government collaboration on a wide range of critical infrastructure security and resilience policy and strategy issues. The U.S. technology industry formed and funds the IT Sector Coordinating Council (IT-SCC) to work closely with the Department of Homeland Security (DHS) to ensure better preparedness and coordination of critical infrastructure protection (CIP) initiatives impacting the sector. Recently, as part of the revised National Infrastructure Protection Plan (NIPP), the IT-SCC collaborated with its GCC partners at DHS to develop and revise a Sector-Specific Plans (SSP) focusing on the unique operating conditions and evolving risk landscape impacting the sector. SCCs across 17 critical infrastructure sectors similarly completed revised SSPs in 2015.

Transportation

The transportation and automotive sectors are one of the most promising beneficiaries of this evolving technology, with a century old industry increasingly looking to the tech industry to innovate and enable new technologies. With the embedding of technology throughout the automobile such that vehicles are now "computers on wheels," already there have been improvements in performance, maintenance, reliability, and most importantly, safety and efficiency. While these advances are present in the marketplace today, the consumer intelligent vehicle marketplace is only in its infancy. Advanced braking assistance, adaptive cruise control, lane departure controls, left-turn assistance, blind spot detection and notification, and parking assistance are a few of the ADAS currently available and increasing in market penetration. The next major jump in smart vehicle capabilities that will fundamentally change the way automobile are utilized will come from advanced cellular and other vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and independent autonomous vehicle capabilities and self-driving cars which utilize different technologies.

The Department of Transportation (DoT), and specifically the National Highway Traffic Safety Administration (NHTSA), have taken steps within their existing authorities to address many areas arising from the increasing amount of technology in today's automobiles, as well as those just on the horizon. Earlier this spring, NHTSA opened a request for comment on security for new and emerging technologies in automobiles to address new potential vulnerabilities as a result of more technology and connectivity in vehicles.[29] ITI, Texas Instruments, the Consumer Technology Association (CTA), and others submitted comments with extensive suggestions in that proceeding.[30] Similarly, NHTSA has taken action within existing authority to address

[29] *See* Department of Transportation, Highway Traffic Safety Administration (NHTSA), Request for public comments Safety Related Defects and Emerging Automotive Technology, Docket ID NHTSA-2016-0040.

[30] ITI believes NHTSA should leverage cybersecurity work that is being done elsewhere in the federal government, much of which is discussed in the above sections, to address security in vehicles. ITI, CTA, and others did express concern that in some areas of the RFC (Docket ID

connected vehicles.[31] In the V2V and V2I space, there are various technologies being tested to deliver these capabilities, and ITI companies are working on each of them. Advanced Long Term Evolution (LTE-Advanced),[32] Dedicated Short Range Communication (DSRC),[33] and fifth generation (5G) wireless technology[34] are all being developed and tested for use in connected vehicle safety applications. Each of these provide specific characteristics needed to reliably enable vehicles to connect with wireless networks, transportation infrastructure, and other vehicles, and low enough latency to provide information in the matter of milliseconds necessary to make critical safety calculations and respond. Given there is clearly not consensus among NHTSA and industry, ITI does not believe NHTSA should move forward with its proposed approach.

Additionally, DoT is helping to facilitate technologies that are slightly further off, namely self-driving vehicles. In this area, DoT and NHTSA's authority is unclear, however, this has not stopped the agency from holding public meetings[35] and updating guidance[36] for the deployment of this technology. We believe this activity is appropriate and helpful to give guidance to industry in moving forward on automated vehicle technology. Lastly, ITI strongly supports DoT's Smart Cities Challenge.[37] DoT has pledged up to $40 million and private funding of up to $10 million will be available to one city to help it fully integrate innovative technologies – self-driving cars, connected vehicles, and smart sensors – into their transportation network.[38] ITI believes this is an excellent approach to allow cities to think outside the box, and

---

NHTSA-2016-0040) NHTSA was reaching beyond its authority to potentially regulate devices and technology connected to vehicles.

[31] *See* NHTSA Advanced Notice of Proposed Rulemaking Vehicle-to-Vehicle Communications, Docket ID NHTSA 2014-0022-0002.

[32] *Cars Talk to Cars on the Autobahn*, IEEE Spectrum, November 10, 2015, http://spectrum.ieee.org/cars-that-think/transportation/infrastructure/cars-talk-to-cars-on-the-autobahn.

[33] *See* Overview of Dedicated Short Range Communication, U.S. Department of Transportation, http://www.its.dot.gov/dsrc/.

[34] Stephen Shankland, *How 5G Will Push a Supercharged Network to Your Phone, Home, Car,* CNet, March 2, 2015, http://www.cnet.com/news/how-5g-will-push-a-supercharged-network-to-your-phone-home-and-car/, and Stephen Lawson, *The Smartest Cars May Need 5G Networks, Ericsson Says*, PCWorld, January 18, 2014, http://www.pcworld.com/article/2089440/the-smartest-cars-may-need-5g-ericsson-says.html.

[35] *See* NHTSA Meetings: Guidelines for the Safe Deployment and Operation of Automated Vehicle Safety Technologies, Docket ID NHTSA 2016-0036-0001.

[36] *See* NHTSA *Guidelines for the Safe Deployment and Operation of Automated Vehicle Safety Technologies*, Docket ID NHTSA 2016-0036-0054.

[37] *U.S. Transportation Secretary Fox Visits All 7 Finalists Cities*, U.S. Department of Transportation, May 16, 2016, https://www.transportation.gov/smartcity.

[38] *U.S. Transportation Secretary Fox Visits All 7 Finalists Cities*, U.S. Department of Transportation, May 16, 2016.

look for new technologies to address decades old problems while the IoT and smart cities market is still maturing and evolving.

VI. Technology – Standards, Spectrum, and Network Infrastructure Require Government Leadership

Many of the foundational elements that drove the development, evolution, and investment in the Internet ecosystem that exists today will be necessary to fully realize the potential of the IoT. Adoption of global, industry-driven, consensus-based standards, investment in network infrastructure, and a pipeline of low, medium, and high frequency spectrum being made available for commercial use will all be necessary to facilitate IoT development.

Standards and Interoperability

As the IoT technology landscape comes more into focus, various global, industry-led standards-setting organizations (SSOs) have formed technical and study groups to ascertain to what extent additional standards development is necessary, including cybersecurity. These are typically international in scope, drawing experts and participation from across the globe and across various industry sectors that will be impacted by and benefit from the IoT. It is important for the Department of Commerce, and more generally, all governments to share their thoughts with these SSOs, and when appropriate, to actively participate.[39]

The Commerce Department and other federal agencies should actively consult with industry regarding when and where to invest its limited time and resources in support of IoT standardization.[40] The Commerce Department should strongly encourage governments to focus their time and resources on participation in and supporting industry-led standardization activities. When multilateral organizations are determined to proceed anyway, the Commerce Department should strongly encourage them to allow full industry participation, and to look to existing or pending global standards before undertaking any activity to engage in standardization activities that may be duplicative of, or even conflict with, global industry-led IoT standards.[41]

Spectrum[42]

Given the IoT is connecting physical objects to the Internet, the increased demand for broadband spectrum will exacerbate an already heavily utilized and scarce resource. Congress, the Federal Communications Commission (FCC), and the National Telecommunications and Information Administration (NTIA) have taken significant steps in recent years to address the spectrum pipeline shortage, but making spectrum available for commercial use must be an ongoing process. The National Broadband Plan, completed in 2010, set the goal of making 500

[39] RFC, question 16.c.
[40] RFC, 20.a., 20.c.
[41] RFC, 20.b.
[42] RFC, 6.a.iii.

megahertz (MHz) of spectrum available by 2020.[43] This is an excellent and commendable goal, and the Broadband Plan was a visionary document in that it laid out a detailed roadmap for improving broadband deployment, access, and investment. While IoT-specific spectrum is not necessary (as various IoT use cases will use various technologies from ZigBee, Bluetooth and WiFi to cellular and Ethernet), the goals for flexible spectrum use laid out in the plan, however, must evolve, and NTIA, the FCC, and other federal agencies must work with industry to determine where technology is going and how much licensed and unlicensed spectrum will be necessary in coming years and decades to meet the demand for exponential increases in connected devices and objects.

Data usage for mobile devices today is growing at a staggering pace. In North America, monthly IP traffic will reach 49.7 Exabytes, essentially 9 billion DVDs worth of traffic.[44] Internet traffic is expected to increase 3.2 fold from 2014 to 2019, 66 percent of which will be carried by Wi-Fi/Fixed networks by 2019. There will be 4.3 billion networked devices by 2019, and machine to machine modules will account for 58 percent of all networked devices.[45] Due to the significant penetration of smartphones into the market, and the ubiquity of fourth generation (4G), the average smartphone user in North America consumes 3.8 GB/month of data.[46] This is expected to grow to 22 GB/month by 2021,[47] with the start of 5G trials in 2016-17 and deployments thereafter. Specifically, in the United States, aggregate mobile data consumption more than doubled between 2014 and 2015, from 338.4 billion MB to 804.2 billion MB.[48]

The IoT will accelerate these trends as well as positive GDP impact, if the United States it plans correctly. The number of connected devices will skyrocket from the combination of increasing connectivity to the Internet, penetration and data usage of not only smart phones and tablets but also vehicles and industrial use cases, and maturing of the IoT. According to some

---

[43] *See* National Broadband Plan, Federal Communications Commission (FCC), 75, https://transition.fcc.gov/national-broadband-plan/national-broadband-plan.pdf.

[44] *Cisco Visual Networking Index: Forecast and Methodology*, Cisco, 2014-2019 White Paper, http://www.cisco.com/c/en/us/solutions/collateral/service-provider/ip-ngn-ip-next-generation-network/white_paper_c11-481360.html.

[45] *Cisco Visual Network Index Forecast Highlights for North America*, http://www.cisco.com/c/en/us/solutions/service-provider/visual-networking-index-vni/vni-forecast.htmlCisco, http://www.cisco.com/c/en/us/solutions/service-provider/visual-networking-index-vni/vni-forecast.html.

[46] *Mobility Report*, Ericson, November 2015, 2, http://www.ericsson.com/res/docs/2015/mobility-report/ericsson-mobility-report-nov-2015.pdf.

[47] *Ibid*., 12.

[48] *Annual Mobile Wireless Industry Survey*, CTIA, May 2016, http://www.ctia.org/your-wireless-life/how-wireless-works/annual-wireless-industry-survey.

estimates, "around 28 billion connected devices are expected by 2021, of which more than 15 billion will be connected machine-to-machine (M2M) and consumer electronics devices."[49]

The Commerce Department, NTIA, FCC, and other agencies that hold or utilize spectrum must work together to make more flexible spectrum available for commercial use; all use cases must be explored to supplement existing supplies, including licensed, unlicensed, shared access, and other use scenarios like increased spectrum sharing. More spectrum must be made available in all frequencies, low, medium, and high. This spectrum should be made available in flexible manner, without designation for any specific purpose; there should not be spectrum made available specifically for IoT. Market forces will drive determinations and investment where spectrum bands meet the need for any given IoT technology. Spectrum and bandwidth preferences for each IoT technology will vary with regard to latency, capacity, time, and other demands that cannot be accounted for at the time spectrum is made available.[50]

The FCC should be commended for significant action in all these areas with its simultaneous activity on the incentive auction, finalizing the regulatory structure for the 3550-3700 MHz (3.5 GHz) spectrum,[51] and moving forward expeditiously on millimeter wave (mmW) bands which will promote innovation and investment in 5G, WiGig, and other advanced wireless technologies in spectrum between 24-71 GHz.[52] With respect to the mmW proceeding, swift action by the FCC will put the United States at least two years ahead of where other nations are for deployment in the 28 GHz band, ensuring continued U.S. leadership in wireless technology. Furthermore, 5G, WiGig, and other advanced wireless technologies will help meet the demand for wireless connectivity that will be driven by the IoT. Engineers expect that 5G networks will be able to handle about 1, 000 times more mobile data than the wireless networks of today[53] and WiGig will enable data transfer rates of up to 7 Gigabytes per second.[54] More focus in all these areas will be needed to meet the demands of consumers, businesses, the technology sector, and all who stand to benefit from IoT technologies and applications.

---

[49] *Mobility Report*, Ericson, November 2015, 10.

[50] It is impossible to determine which connective technology may be appropriate for any given IoT application, but certainly Bluetooth, WiFi, 5G, 4G, 3G, and Ethernet, among many others will certainly all be utilized. As such, designating IoT spectrum would not be useful, and would likely result in inefficient use of this limited resource.

[51] *Continuing Momentum in the 3.5 GHz Band*;, FCC, May 17, 2016, https://www.fcc.gov/news-events/blog/2016/05/17/continuing-momentum-35-ghz-band.

[52] *See* FCC Notice of Proposed Rulemaking, 15-138.

[53] *Why IoT needs 5G*, IEE Spectrum, May 20, 2015, http://spectrum.ieee.org/tech-talk/computing/networks/5g-taking-stock.

[54] Ian Paul, *WiGig Group Steps Closer to Making 7 Gbps Wirless a Reality*, TechHive, by Ian Paul, May 10, 2010, http://www.techhive.com/article/195930/Superfast_WiGig_Wireless_Standard_Debuts_FAQ.html.

Network Infrastructure[55]
Robust investment in high quality, high penetration fixed and mobile wireless broadband infrastructure will be necessary to meet the demand for exponential growth in connected devices. This will be especially true as the leap-forward innovative 5G technologies (next generation after today's 4G), in particular, will rely on significantly more cellular antennas than are required for former generations of wireless technology.

A significant impediment to private sector deployment of broadband networks in general is access to existing infrastructure. This can include access to utility poles and conduit, as well as cellular tower and equipment placement. As ITI commented in the NTIA's Broadband Opportunity Council proceeding last year, there are a number of steps that could be taken to address this; among these suggestions were: 1) aggregating reliable information about the status of existing infrastructure, 2) provide that information in a transparent, and uniform format, 3) condition federal funds to require recipients to meet certain conditions on access to their infrastructure for purposes of broadband deployment, and 4) promote "dig once" policies to ease deployment of fiber optic cable.[56] Furthermore, establishment of a unified policy for rights of way access by the Bureau of Land Management (BLM), and by the Federal Highway Administration (FHWA) would further ease burdens when deploying broadband networks on or over the land and infrastructure controlled by these entities.[57]

VII. Federal Agencies Can Derive Significant Benefits and Value from Adopting IoT[58]

The Commerce Department, in developing a strategy to address fostering the advancement of IoT technologies, should examine how the federal government can benefit and leverage the IoT to meet agencies' missions, improve efficiency and effectiveness, process data for better decisions, and create new services to deliver to the public. Many federal agencies are in the early stages of figuring out how to take advantage of IoT technologies and bring these tools to the front line. According to the Govini Internet of Things: Sensors & Data Collectors report, federal IoT spending from fiscal year 2011 to fiscal year 2015 was around $35 billion. The Department of Defense (DoD) is leading the way in military spending, while National Aeronautics and Space Administration (NASA) and DHS are the leading federal civilian agencies. IoT technologies present federal agencies with an enormous opportunity to work with the tech industry to transform government and meet future mission challenges. Industry would encourage greater engagement and partnership with the private sector to understand and leverage the benefits of these new technologies.

[55] RFC, questions 6.a.iv., 7, 8, 9, 10.
[56] *See* ITI Comment to NTIA, Docket No. 1540414365-5368-01/RUS RIN 0660-XC019.
[57] *Ibid*.
[58] RFC, 28.

VIII. Conclusion

ITI appreciates the opportunity to comment in this proceeding, and strongly supports leadership from the Commerce Department and the NTIA in guiding the governments work on the underlying policy issues that will ultimately impact IoT investment, development, and potential. As has been captured above, as well as in the RFC, many if not most policy issues that will impact the IoT are issues the Commerce Department and NTIA have extensive knowledge and experience working on, and ITI looks forward to continuing to collaborate on the administration's work in these areas.

Respectfully submitted,

J. Vince Jesaitis
Vice President, Government Affairs

John Miller
Vice President, Global Policy and Law, Cybersecurity and Privacy

Karolina Filipiak
Manager, Government Affairs

ITI - Information Technology Industry Council
1101 K Street NW, Suite 610
Washington, DC 20005
202-737-8888
www.itic.org