Before the
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
DEPARTMENT OF COMMERCE
Washington, D.C. 20230

In the Matter of	)	
	)	
The Benefits, Challenges, and	)	Docket No. 160331306-6306-01
Potential Roles for Government in	)	RIN 0660-XC024
Fostering the Advancement of the	)	
Internet of Things	)	

COMMENTS OF CISCO SYSTEMS, INC.

Cisco Systems, Inc. ("Cisco") welcomes the opportunity to provide input to the Department of Commerce on issues raised by the National Telecommunications and Information Administration's ("NTIA") request for comments (the "Request") regarding "the benefits, challenges, and potential roles for the government in fostering the advancement of the Internet of Things" (the "IoT").[1]

The IoT holds tremendous promise to transform and improve our lives. The rapid expansion of new technologies and capabilities, however, brings new technical, legal, and policy challenges to the forefront. For example, systems and devices must be interoperable in order to effectively communicate with one another. Adequate spectrum and bandwidth must be available to ensure reliable and fast connectivity and the timely transmission of data. Conflicting legal regimes must be reconciled to allow data to cross borders freely. Horizontal, multistakeholder, public-private partnerships can improve security without exacerbating the problem of conflicting regulatory obligations built around existing industry verticals. The collection, use, analysis and

[1] The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things, 81 Fed. Reg. 19956 (Apr. 6, 2016) ("Request").

storage of vast amounts of data require management of attendant risks. And we must train our workforce with the technical skills needed to foster and deploy innovations in the IoT landscape.

There is no doubt that the advancement of the IoT will require unprecedented coordination among a myriad of government and industry stakeholders, substantial investments in technology and infrastructure, and a flexible and supportive regulatory and policy environment. As with any emerging technology, however, with new challenges comes room for regulatory mischief. As discussed in more detail below, there are many potential touchpoints in the IoT ecosystem for regulators and policymakers. Their decisions could, quite literally, make or break the evolution of the IoT. Unfortunately, the risk of overregulating or promulgating inconsistent regulations runs high.[2] Regulators and policymakers must be both cautious and humble in their oversight of this nascent sector. Agencies must consult and coordinate with each other to ensure that existing vertical regulations that may be applicable to the IoT technologies do not conflict or create undue burdens on innovators. While application of existing sector-specific regulations to certain uses of IoT technologies may make sense, particularly where there are unique public safety or other imperatives (*i.e.*, self-driving cars and drones), it often will not. Even when this is true, we must be careful to avoid requirements that render these technologies incapable of being adapted and updated efficiently in a dynamic threat environment. More likely, however, the development of flexible, industry-led, consensus-based standards and best

[2] For example, at least 41 states have considered legislation related to unmanned aircraft systems ("UAS" or "drones"), while the Federal Aviation Administration ("FAA") has issued a proposed rulemaking specifying requirements for the operation of UAS. *See* National Conference of State Legislatures, *Current Unmanned Aircraft State Law Landscape* (May 19, 2016), http://www.ncsl.org/research-/transportation/current-unmanned-aircraft-state-law-landscape.aspx. Likewise, at least 15 states have considered legislation for self-driving cars. *See* Andy Szal, *Google Official Calls for Nationwide Autonomous Vehicle Regulations*, Manufacturing Business Technology (Apr. 29, 2016), http://www.mbtmag.com/news/2016/04/google-official-calls-nationwide-autonomous-vehicle-regulations.

practices that leverage multi-stakeholder, public-private partnerships will yield more effective management of cybersecurity risks.

At the same time, there is a role for government in certain instances. For example, the government can work with industry stakeholders to promote interoperability. It can design policies to promote the adequate availability of spectrum. It can consult with our international neighbors to ensure the free flow of cross-border data. Perhaps the most critical function of the government, however, is to ensure that our education policies and resources are properly focused on the promotion of STEM education. If there is but one role that the government should play in the IoT space, this is it. For without an educated and well-trained workforce, the advancement of the IoT will stutter.

Cisco commends the NTIA for providing a platform to engage in a cohesive dialogue in an otherwise disparate IoT landscape. We also applaud the NTIA and the Department of Commerce more broadly for its understanding that policies aimed at harnessing market forces and leveraging strategic public/private partnerships will more effectively incentivize managing privacy and safety risks than the development of a new wave of "IoT regulations."

I. INTRODUCTION

The Internet has revolutionized the world around us – transforming the way that we use and share data to communicate, collaborate and consume entertainment and information. Yet, the next wave of technology is not just about moving data from one place to another. Rather, it about connecting physical objects to the Internet on an unprecedented scale.

Cisco has always been about making connections. Since 1984, it has been exploring the possibilities that arise from connecting the unconnected. Several years ago, Cisco began a discussion about the next wave of the Internet – a digitized world where the networked connections of people, process, data and things are brought together to unlock unprecedented

value, offering new types of data and insight, and blending physical and virtual environments seamlessly for great business and societal outcomes. Cisco has worked with innovative partners around the world to build and implement digital roadmaps that will transform industries from manufacturing to retail to government. The IoT holds incredible promise, potentially injecting trillions of dollars in value into the U.S. economy over the next decade, driven by efficiencies and advancements realized across a variety of industries and settings. For instance:

- Utility companies will be able to gain deeper levels of insight into demands placed on the grid, allowing for better energy management and generating savings;

- Brick-and-mortar retailers will use multiple data points from a variety of sources about customer behavior to make more informed decisions about inventory, pricing, and customized offerings;

- Putting more networked devices on the factory floor will allow manufacturers to more quickly detect issues and repair manufacturing processes;

- Patients will be able to share their health data such with their doctors in real time through wearables, allowing for the quicker detection of any health abnormalities, such as cardiac issues, and facilitating early intervention; and

- Farmers will use sensors that will provide updates on soil composition, temperature and water levels, ensuring efficient use of resources.

These are but a few examples of how IoT applications can help maximize efficiencies, reduce waste, and generate value. The possibilities are nearly limitless.

While the Request asks a host of questions, they break into three groups: 1) what is the IoT; 2) what are the opportunities associated with adoption of the IoT and challenges that would prevent the growth of this market segment; and 3) which challenges and opportunities identified require a significant governmental role. Cisco offers its thoughts on each below.

II. DISCUSSION

A. *DEVELOPING A COMMON DEFINITION OF THE IOT*

As a threshold issue, the Request asks whether a common definition should be used in examining the IoT landscape and why.[3] At its most basic level, the IoT links "smart" objects to the Internet and to each other, facilitating the conversion of data gathered by sensors into usable intelligence and enabling that intelligence to reach the right person or machine. In Cisco's view, some definitions of the IoT have been overly constricted by their focus on interactions between people and sensors. We believe the lens should be wider and include the full range of networked connection involving people, process, data and things. In this vision, IoT encompasses machine-to-machine ("M2M"), machine-to-person ("M2P"), and person-to-person ("P2P") connections in addition to the interactions between people and devices.

B. *THE IOT HOLDS INCREDIBLE PROMISE*

The Request seeks comment on the most significant new opportunities and/or benefits created by the IoT.[4] In short, the value to be gained by the IoT is nothing short of astonishing. According to a Cisco study, over the next decade there is a $14.4 ***trillion*** "Value at Stake" in the IoT for the private sector and $4.6 trillion for the public sector.[5] By Value at Stake, Cisco is referring to new economic value that can be captured by connecting things, processes, data, and

---

[3] Request, 81 Fed. Reg. at 19958.

[4] *Id*.

[5] Joseph Bradley et al., *Internet of Everything (IoE): Top 10 Insights from Cisco's IoE Value at Stake Analysis for the Public Sector*, at 2 (Cisco Economic Analysis 2013), http://www.cisco.com/c/dam/en_us/about/ac79/docs/IoE/IoE-VAS_Public-Sector_Top-10-Insights.pdf and Joseph Bradley et al., *Embracing the Internet of Everything To Capture Your Share of $14.4 Trillion: More Relevant, Valuable Connections Will Improve Innovation, Productivity, Efficiency & Customer Experience*, at 2-3 (Cisco White Paper 2013) ("Cisco White Paper"), https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoE_Economy.pdf. The figures do not include potential Value at Stake from the consumer sector, or from societal benefits generally, and were calculated by identifying values that would be generated between 2013-2022.

people – economic value that is not achievable in an unconnected society. No doubt connections are growing. Between 2014 and 2019, there will be one billion more Internet users and 10 billion more IP-connected devices, with M2M devices driving growth and making up more than 40% of the total connections by 2019.[6] A good way to look at the potential demand is that only 0.6% of all the objects that may one day be connected are connected today.[7] The task is to use that enhanced connectivity for the betterment of society.

The IoT is being driven by several factors:

- *First*, powerful technology trends – including the dramatic increase in processing power, storage, and bandwidth at ever-lower costs; the rapid growth of cloud, social media, ad mobile computing; the ability to analyze Big Data and turn it into actionable information; and an improved ability to combine technologies in more powerful ways – make it possible to realize more value from connectedness.
- *Second*, barriers to connectedness continue to drop. For example, IPv6 creates enough address capacity for every star in the known universe to have 4.8 trillion addresses.
- *Third*, form factors continue to shrink. Computers can be the size of a grain of salt, and sensors can be the size of a speck of dust, used to communicate temperature, pressure, and movement.
- *Fourth*, the IoT reflects the reality that business value creation has shifted to the power of connections and the ability to create intelligence from those connections.[8]

[6] Jeff Campbell, *The Internet of Things*, at 4, Cisco (Apr. 25, 2016) (on file with author).

[7] Cisco, *The Internet of Everything: Cisco IoE Value Index Study*, at 1 (Cisco Frequently Asked Questions 2013), http://internetofeverything.cisco.com/sites/default/files/docs/en/ioe-value-index_FAQs.pdf.

[8] Cisco White Paper at 2-3.

Technology and business trends are creating unprecedented opportunity to connect the unconnected, and to realize new efficiencies across industries. Values can be generated in a variety of settings, such as factories, cities, homes, offices, schools, vehicles, retail environments, industrial sites, and on the human body.[9] But how is value calculated and derived from these technological innovations? Cisco has defined the "Value at Stake" as the potential bottom-line value (higher revenues and lower costs) that can be created or will migrate among companies and industry based on their ability to harness the IoT.[10] Values in the private and public sectors are realized differently and thus are addressed separately below.

1. PRIVATE SECTOR VALUE AT STAKE

Cisco analyzed more than 50 "use cases" in the private sector to calculate the value generated by IoT deployment and concluded that those that harness the potential of the IoT will do so by either capturing new value created from technology innovation or by gaining competitive advantage and grabbing market share from competitors who have not capitalized on the IoT's capabilities.[11]

Looking across industries in the private sector, the greatest value from the IoT is primarily derived from five drivers: (1) asset utilization (reduced costs from improved business executions and improved capital efficiencies); (2) employee productivity (greater labor

[9] James Manyika et al., *The Internet of Things: Mapping the Value Beyond the Hype*, McKinsey Global Institute, at 3 (June 2015) ("McKinsey Study").

[10] Bradley, *supra* note 8, at 3. For example, Cisco calculated the Value at Stake for its "Connected Commercial Ground Vehicles" use case by considering (1) lower costs for fleet owners, and (2) potential revenue increases for service providers. Based on its analysis fuel efficiencies and driver productivity driven by IoT applications, it calculated the annual benefits to be at $970 annually per vehicle. The analysis also calculated new revenue opportunities for service providers generated by IoT applications, such as connectivity and other value-added services, at $12-$15 monthly. The overall Value at Stake number - $347 billion – reflects the net present value of the benefits for fleet owners and service providers over a 10-year period. *Id.* at 17.

[11] *Id*. at 3-4.

efficiencies); (3) supply chain and logistics (eliminating waste in the supply chain); (4) customer experience (addition of more customers), and (5) innovation (improved R&D speeds, reducing time to market, and new business models).[12]

Broken down by industry, the manufacturing sector stands the most to gain from the adoption of IoT, with connected factories representing an estimated value of up to $1.95 trillion derived from increased productivity, energy savings, equipment maintenance, and inventory optimization.[13] Take the King's Hawaiian company, which produces sweet dinner rolls. After installing eleven new IoT connected machines, King's Hawaiian was able to put out an additional 180,000 pounds of bread every day. The machines were linked to FactoryTalk, software that lets the company's employees have remote access to both historical and real-time data and features production dashboards that provide a comprehensive picture of the whole system so they can monitor performance. The new technology has increased efficiency, improved asset utilization, and lowered maintenance costs.[14]

---

[12] Cisco, *Internet of Everything (IoE): Value at Stake in the IoE Economy*, at 8 (2013), http://www.slideshare.net/fullscreen/CiscoIBSG/internet-of-everything-ioe-economy/1.

[13] *Id*. at 7. It is worth noting that the McKinsey study puts the value at a higher number – claiming that the adoption of IoT applications in factory settings could generate an economic impact of $1.2 trillion to $3.7 trillion per year by 2025. McKinsey Study at 8. The McKinsey study defines factories broadly, however, to include all standardized production environments, including agricultural and hospital settings as well as traditional manufacturing environments. McKinsey Study at 8.

[14] Kylie J. Wakefield, *How The Internet Of Things Is Transforming Manufacturing*, Forbes (July 1, 2014), http://www.forbes.com/sites/ptc/2014/07/01/how-the-internet-of-things-is-transforming-manufacturing/#1e76c898228e. A joint solution of Bosch, Cisco, and Mahindra illustrates another example of the IoT in action. These companies worked together to connect power tools into a system for tightening industrial fasteners (nuts, bolts, rivets, screws) with the correct amount of torque and speed while also capturing data for real-time analysis to drive accuracy, quality and safety. The result is improved accuracy by recording torque data for hundreds of thousands of bolts, which allows manufacturers to (1) identify discrepancies and potential causes of faults; (2) minimize worker error; (3) power down tools when used incorrectly; (4) improve processes and productivity in real time to detect problems. *See* Cisco, Customer Success Stories, *Powering Manufacturing Precision*, http://www.cisco.com/c/m/en_us/ioe/digital-transformation-stories/index.html#/story?storyId=110 (last visited May 31, 2016).

The marketing and advertising industry also stands to be a key beneficiary of the IoT, with a $1.95 trillion of total Value at Stake.[15] Today, it is very difficult to create and implement cohesive advertising channels (TV, radio, Internet, point of sale) and to accurately assess/predict consumer behavior in brick-and-mortar stores. By placing sensors in the retail environment, companies will be able to use analytics about consumer shopping patterns in a way that online retailers have enjoyed for years.[16] They will have a complete view of their customers and allow them to react to their markets in real time, based on a holistic assessment of customers' wants and needs.[17] For example, Mayland Real Estate deployed Cisco Connected Mobile Experiences ("CMX") solutions so that guests could receive free Wi-Fi from anywhere in its two-story Centrum Riviera complex. Leveraging analytics through CMX, Centrum Riviera can collect anonymized data about its shoppers, including their behavior patterns, whether it is their first visit, and the duration of their stay. This data, which is collected, protected, and used in accordance with the law, allows Maryland Real Estate to evaluate the effectiveness of their

[15] Bradley, *supra* note 8, at 8.

[16] *Id.* at 17. The 18 industries measured for the amount of Value at Stake, in order of size, include: (1) manufacturing; (2) retail trade; (3) information services; (4) finance and insurance; (5) healthcare; (6) educational services; (7) professional scientific, and technical services; (8) administrative and waste management services; (9) wholesale trade; (10) arts, entertainment, and recreation; (11) other services (excluding government); (12) agriculture, fishing and hunting; (13) construction; (14) transportation and warehousing; (15) management of companies and enterprises; (16) real estate, rental and leasing; (17) mining; and (18) utilities.

[17] Of course, technologies in this space must be engineered with privacy and security in mind. As discussed below, traditional notions of data protection (i.e., notice and choice) are still very relevant in the context of the IoT but present challenges where the devices gathering data may lack screens, keyboards, or other user interfaces. The industry is actively engaged in addressing privacy issues as these technologies, consumer awareness and understanding of them, and existing regulatory obligations for data protection continue to evolve.

marketing programs, and allows Centrum Riviera tenants to anticipate shopper traffic, schedule store staffing, and understand the amount of time its customers spend in their stores.[18]

2. PUBLIC SECTOR VALUE AT STAKE

The public sector also has much to gain by the deployment of the IoT across the spectrum, including in education, culture and entertainment, transportation, safety, healthcare and defense. The four primary drivers of the IoT's value in the public sector are: (1) employee productivity (improved labor effectiveness) and connected defense (improved situational awareness and connected command centers, vehicles, and supplies); (2) cost reduction (improved labor efficiency and reduced operational costs); (3) citizen experience (improved environments and better health outcomes); and (4) increased revenue (improved ability to match supply with demand; improved monitoring and compliance).[19] More than two-thirds of the $4.6 trillion value will be driven by P2P or M2P connections, such as telework, connected learning, and travel avoidance (P2P) and video surveillance, smart parking, and disaster response (M2P), respectively.

Cities will generate almost two-thirds of the IoT's benefits to civilian governments globally.[20] To maximize the value, cities should employ strategies that combine water management, smart grid, waste management, particulate monitoring and gas monitoring in a

[18] Cisco, *Digital Transformation with the Internet of Everything: 100 Customer Stories*, at 143 (2016), http://www.cisco.com/c/dam/m/en_us/ioe/digital-transformation-stories/digital-transformation-with-the-internet-of-everything.pdf; *see also* Cisco, *Mall Learns About Shopper Behavior from Location Information* (Cisco Customer Case Study 2014), http://www.cisco.com/c/dam/en/us/products/collateral/wireless/mobility-services-engine/riviera-shopping-center.pdf.

[19] Bradley, *supra* note 5, at 2-3.

[20] Cities will claim 63% of the IoT's total civilian benefits over the next decade, as compared to 22 and 15% claimed by states and the federal government, respectively. *See id.* at 4.

comprehensive fashion, rather than addressing each piecemeal. Cooperation across city functions and departments, including resource sharing, will be essential.

The IoT is already delivering value in the public sector. For example, thanks to a fiber-optic network backbone and wireless mesh network that extends connectivity throughout the city, the City of San Antonio has developed a variety of IoT-based capabilities, including a networked traffic-light system that allowed it to recoup an estimated $2 billion that was lost due to longer commutes, higher fuel expenses, safety issues and other factors. Likewise, Barcelona's Smart City encompasses 83 projects across 12 different service areas, including a smart water program. Together these projects deliver millions in annual savings, annual increases in revenues from connected technologies such as smart parking, and thousand new jobs.[21]

A Kansas City smart city project developed in conjunction with Sprint, GE, and Sensity is another significant example of the IoT in action.[22] In May 2014, Kansas City, Missouri partnered with Cisco and others to design a smart city platform that would "enhance Internet connectivity, enable efficiencies in management of public infrastructure, introduce new revenue streams, and ultimately improve the citizen experience."[23] Included in the design is smart lighting to ensure safer streets, and more efficient management of roads, bridges and city assets through use of data and analytics gathered from sensors placed along the streetcar starter line in the downtown area. Because we cannot always anticipate all the potential benefits that will flow from the connections enabled via IoT, the project also includes a Living Lab where new uses for

---

[21] Joseph Bradley et al., *Internet of Everything in the Public Sector: Generating Value in an Era of Change Top 10 Insights*, at 11 (Cisco Study Findings 2014), http://www.cisco.com/c/dam/assets/global/RU/tomorrow-starts-here/pdf/Public_Sector_FULL_REPORT-EN_RU.pdf.

[22] Kansas City Living Lab, http://kclivinglab.com/ (last visited May 31, 2016).

[23] Kansas City Living Lab, Project Overview, http://kclivinglab.com/program-overview/ (last visited May 31, 2016).

the data collected through the project can be proposed. Using the city as an incubator drives innovation, speeds up the commercialization of new technologies, and enhances the quality of life of the city's residents.[24]

3. CONSUMER BENEFITS OF THE IOT

The ultimate beneficiaries of the IoT, of course, are people – citizens will enjoy greater health, reduced commuting times, better work environments, greater savings on energy, enhanced retail experiences. Consumer-facing IoT applications, which will help drive $287 billion in tech retail sales in 2016,[25] will connect to make our homes safer, our appliances more efficient, and our chores less burdensome. In the wearables market alone, the possibilities are endless: virtual reality goggles that provide for immersive education; sports helmets to alert the team physician to a possible concussion; GPS-enabled slippers to make sure an elderly relative doesn't wander off. Put simply, the IoT will allow us all to enjoy longer, healthier, and higher quality lives.[26]

C. *CHALLENGES TO THE ADOPTION OF THE IOT*

Despite its budding success, the IoT landscape faces both technical and policy challenges – and they are not mutually exclusive. As observed in the Request, technology is "at the heart" of the IoT.[27] Thus, to enable its development, issues relating to reliability, scaling, power, connectivity, and capacity must be resolved. Frameworks need to be developed that will address

[24] ThinkBig, http://thinkbigpartners.com/ (last visited May 16, 2016).

[25] Press Release, Consumer Technology Association, *IoT Will Drive Consumer Tech Industry to $287 Billion in Revenues, an All-Time High, According to Consumer Technology Association* (Jan. 4, 2016), http://www.cta.tech/News/News-Releases/Press-Releases/2015-Press-Releases/IoT-Will-Drive-Consumer-Tech-Industry-to-$287-Bill.aspx.

[26] Sarah Hedgecock, *New Report Tempers Rosy Outlook For Wearable Health Devices*, Forbes (Oct. 27, 2014), http://www.forbes.com/sites/sarahhedgecock/2014/10/27/new-report-tempers-rosy-outlook-for-wearable-health-devices/#38ab6f126fb6 (survey participants believed that use of wearables would extend their lifespan by a decade).

[27] Request, 81 Fed. Reg. at 19958.

standards and interoperability, security and privacy, and spectrum and bandwidth constraints. International coordination to allow for cross-border data flow is essential to capturing the full value of the IoT. Intellectual property and product liability laws must be carefully applied in a manner that will not impede innovation. And policies must be in place to promote the training and education of our workforce.

Tackling these challenges is no easy task, given the wide diversity in the IoT ecosystem in terms of devices, applications and industries. It is further compounded by the fact that numerous federal agencies are already vying for a piece of the action – the risk of over-regulation is very real. As discussed below, a light regulatory touch with a focus on multi-stakeholder partnerships, including both industry and government stakeholders will bring us closer to realizing the vision of a super-connected world where cybersecurity and data protection risks are appropriately managed.

i. Adoption of Open Standards

As the Request rightly notes, interoperability is a key challenge to the development of the IoT.[28] The IoT, like the Internet, is a network of networks.[29] But, there are different requirements for different networks. While the IoT is a useful overarching term, it does not reflect the multiplicity of different requirements and the resulting architectures. For example, cost considerations may suggest that for many low-bandwidth IoT applications, wireless air interface standards like LTE developed for consumer voice and data services may not be the right choice. Likewise, the enterprise-specific networks of utilities, for example, present very different regulatory issues than open networks that invite public use (*e.g.*, monitoring parking

[28] *Id*. at 19959.

[29] Dave Evans, *The Internet of Things: How the Next Evolution of the Internet Is Changing Everything*, at 4 (Cisco White Paper 2011), http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

space availability). While one may have a smart meter at home as well as a bio sensor, they have no need to communicate with each other, they are managed (and may belong) to different entities and while one can be attached to a private infrastructure the other may go over the public internet. Nevertheless, Internet Protocol (IP) is becoming the common language for most data communications, including that related to IoT. Proprietary networks are migrating to IP in sectors such as the electricity grid, building systems, industrial manufacturing and oil systems. Enterprises are recognizing the value of interoperability and scale, while IP networks have evolved to handle reliability demands.

To maximize the benefit of the IoT, silos between technologies must be broken down to unlock the value for the economy and society.[30] Agreeing on a wide range of open standards maximizes economies of scale and simplifies education requirements. Standards that are accessible to prospective implementers are key to driving interoperability, and the consequent benefits for the quality and capabilities of analytics.[31] Without interoperability, it has been posited that at least 40% of the benefits of the IoT will not be realized,[32] and the IoT will turn into a lesser Internet of *Some* Things. Cisco is committed to the goal of maximizing interoperability, and together with other major industry players launched the Industrial Internet Consortium,[33] and has been heavily engaged in the setting up of the Alliance of IoT for Innovation[34] in order to help make this reality.

---

[30] Request, 81 Fed. Reg. at 19959.

[31] Connected cars provide a prime example of the importance of interoperability. A car is manufactured with connected parts using one standard. But what about other cars, traffic lights, or sensors detecting traffic patterns? If all of these components are speaking different languages, so to speak, then they will not be able to speak to each other, greatly reducing the benefits of the IoT.

[32] McKinsey Studay at 11.

[33] *See* Industrial Internet Consortium, http://www.iiconsortium.org (last visited May 31, 2016).

[34] *See* Alliance for Internet of Things Innovation, www.aioti.eu (last visited May 31, 2016).

Standard setting should be driven by industry using current standards development organizations with the aim of setting a global framework. The nature of the IoT demands that a variety of different standards, including wireless, technical, application, quality and compliance standards, will be implicated, and thus a variety of different standard setting organizations will be involved.[35] The role of government should be to encourage the development and adoption of open standards relating to IoT, and to foster interoperability through open and transparent processes. But the government should avoid "picking winners" from among different standards. The government should participate in standards setting activities as a convener, as a trusted expert, and as a major purchaser of technology and implementer of standards. However, the government should continue to heed the important requirements of the National Technology Transfer Act of 1995 and the OMB Circular A-119, which emphasize the importance of government reliance on voluntary, consensus based standards versus technical requirements set by the government.

The widespread adoption of IoT will require large numbers of inexpensive devices that implement communications-related interoperability standards (such as LoRa, Zigbee, Wi-Fi, and LTE). For example, adoption of smart water and power meters that can communicate usage information to a utility through a cellular network will be discouraged if the addition of the cellular modem to a meter significantly increases the cost of the meter to the utility or ratepayer. The issue of licensing costs associated with the implementation of interoperability standards used in wireless devices is therefore important to the success of the IoT.[36] There have been promising

[35] Among the standard setting organizations already involved in IoT-related activities are ATIS, CEN, CENELEC, Continua Alliance, ETSI, 3GPP, IEC, IETF, ITU-T (SG13 for y.IOT work), IEEE, IPSO, OneM2M and W3C.

[36] For further background, *see* Keith Maskus & Stephen A. Merrill, *Patent Challenges for Standard-Setting in the Global Economy: Lessons from Information and Communication Technology* (2013);

developments in US courts and in the positions taken by US competition enforcement agencies regarding limiting the ability of owners of patents essential to implement telecommunications interoperability standards to compel payment of super-competitive licensing terms by wielding the threat of injunctions and other prohibitive orders.[37] This is an area that merits continued attention from policymakers concerned with the success of IoT.

Related issues worthy of continued attention include providing implementers of IoT standards and patent licensors with greater transparency and predictability regarding licensing costs, and industry concerns with the stacking of royalties for patents required to implement interoperability standards.[38] Both issues aim at addressing the risk that patent licensing costs, may form a significant cost barrier to the widespread adoption of IoT by utilities, public authorities, and others. Implementing standards may require licenses to a wide range of patents. As patents are increasingly acquired by non-practicing entities whose only business is patent licensing, more patentees owning patents required to implement interoperability standards focus on maximizing royalty income rather than, for example, defensive use of patents. This threatens to make patent licensing costs a barrier to adoption of IoT solutions, as the potential cost are huge (for example, IoT deployments to sense traffic patterns in large metropolitan areas or power flow across the electrical grid of a distribution network may require the acquisition of millions of sensing devices).

International Telecommunications Union, *Understanding parents, competition and standardization in an interconnected world* (2014), http://www.itu.int/en/ITU-T/Documents/Manual_Patents_Final_E.pdf.

[37] *See Apple, Inc. v. Motorola, Inc.* 757 F.3d 1286, 1331-33 (Fed. Cir. 2014); US Department of Justice and US Patent and Trademark Office, *Policy Statement on Remedies for Standards-Essential Patents Subject to Voluntary F/RAND Commitments* (Jan. 8, 2013), http://www.justice.gov/atr/public/-guidelines/290994.pdf.

[38] *See e.g.*, Ann Armstrong et al., *The Smartphone Royalty Stack: Surveying Royalty Demands for the Components Within Modern Smartphones*, at 69 (Working Paper), https://www.wilmerhale.com/-uploadedFiles/Shared_Content/Editorial/Publications/Documents/The-Smartphone-Royalty-Stack-Armstrong-Mueller-Syrett.pdf.

Clarity around licensing costs will facilitate widespread implementation of standards, while continued uncertainty around licensing costs will discourage it. Courts in the U.S. have rigorously applied methodologies that account for royalty stacking concerns and have set royalties at a fraction of what patent holders have sought.[39] This is an area that also merits continued attention.

ii. More Network Bandwidth, Reasonable Traffic Management, and Adoption of IPv6

With more devices being connected, the need for more bandwidth increases.[40] While the average PC traffic will almost double to 39.2GB per month in 2018, the average M2M module will create almost 7 times the amount of traffic by 2018 at 514MB. Coupled with the expansion in the number of devices, the traffic will be 22 times greater in 2018 than 2013. This expansion in traffic dictates the need for greater network bandwidth – and smarter use of the bandwidth that is available. To meet this demand, policymakers need to create the right framework to stimulate investment in more robust and higher speed broadband networks, both wired and wireless, fixed and mobile.

But IoT will require more than just bandwidth – it will require the ability to handle different feature requirements of traffic flows, from low latency for bidirectional high definition video to coping with data bursts for wireless data transfer. There will be an increased need for network resource management tools to handle the connected devices, their feature requirements,

[39] For example, *Microsoft Corp. v. Motorola, Inc.*, 2013 U.S. Dist. LEXIS 60233 (W.D. Wash. April 25, 2013); Memorandum Opinion, Findings, Conclusions, and Order, *Innovation IP Ventures, LLC*, Case No. 11 C 9308 (N.D. Ill., Oct. 3, 2013).

[40] Request, 81 Fed. Reg. at 19959.

and the data they produce. Diverse network traffic must be appropriately managed and there must be room for further innovation through managed or specialized services.[41]

Finally, there is the issue of IP addresses. There is no doubt that IPv6 will be the internet protocol for the IoT. With only 4.3 billion IPv4 addresses, many devices already have to share IP addresses. The stock of IPv4 addresses has simply run out. This is a problem, given that billions of new connected devices will be added to the IoT ecosystem in coming years (and will need IP addresses). Presently, IPv4 has been hanging on by a thread with the help of network address translation ("NAT") and carrier-grade network translation ("CGNAT").[42] NAT and CGNAT are used to essentially cheat the system and allow multiple devices to share one IP address.[43] While these system tricks have allowed for the "extended life-support for IPv4 for almost two decades" there are downsides.[44] When one user in a group of users sharing an address does bad things, for example, identifying abusers becomes almost impossible.[45] Moreover, not only is the use of NATs as a solution for limited IP addresses expensive to maintain, it also creates multiple interoperability issues with applications and devices.[46]

---

[41] To that end, the Federal Communications Commission ("FCC") should be prepared to apply its principles of Net Neutrality in a manner that will facilitate the promotion of IoT deployment. *See* Monica Alleven, *Net neutrality: Long-term implications loom for Internet of Things*, Fierce Wireless Tech (Feb. 26, 2015), http://www.fiercewireless.com/tech/story/net-neutrality-long-term-implications-loom-internet-things/2015-02-26.

[42] Scott Hogg, *ARIN Finally Runs Out of IPv4 Addresses*, Network World (Sept. 22, 2015), http://www.networkworld.com/article/2985340/ipv6/arin-finally-runs-out-of-ipv4-addresses.html.

[43] Geoff Huston, *An Update on IPv6*, Circle ID (June 21, 2015), http://www.circleid.com/posts/-20150621_an_update_on_ipv6/.

[44] Hogg, *supra* note 40.

[45] Girish Managoli, *8 Reasons to make the switch to IPv6*, Opensource.com (Jan. 2016), https://opensource.com/business/16/1/scale14x-interview-owen-delong-akamai-technologies.

[46] *Id. See also* Hogg, *supra* note 40.

By accelerating the move to IPv6, these issues are resolved.[47] IPv6 is beyond the realm of foreseeable exhaustion. There are enough addresses for every atom on the surface of the Earth to have 100 addresses. Transitioning to IPv6 will allow the IoT to continue to grow and prevent address exhaustion from acting as a bottleneck, squeezing innovation.

Policymakers need to champion IPv6 adoption in networks, devices, and websites, and promote more IPv6 enabled content. The NTIA has previously identified three potentially helpful government activities that may support the development and deployment of IPv6.[48] First, the government could support certain types of research and development activities. Organizations such as NIST and the NTIA are ideally positioned to foster industry/government collaboration in areas such as mobile IPv6 routing, security in dual-stack environments, and privacy implications of IPv6. Second, the U.S. government can act as a consumer of IPv6 products and services. Federal agencies could lead by example as being an early adopter of IPv6. Finally, the government can act as educator. Federal agencies can conduct awareness campaigns to promote the adoption of IPv6. The government can also offset some of the costs associated with the cost of IPv6 deployment by actively supporting and funding training opportunities to get engineers and technology professionals up to speed with the technical knowledge or expertise necessary to handle the specifics of IPv6 implementation.

iii. Addressing Spectrum Requirements

Given the rapid growth in traffic and the increasing number of devices, there will undoubtedly be a need for more spectrum. The following statistics on M2M connectivity in North America paints a stark picture of its urgency:

---

[47] Managoli, *supra* note 43. *See also* Hogg, *supra* note 40.

[48] *See* NTIA, IPv6 Task Force, *Technical and Economic Assessment of Internet Protocol Version 6 (IPv6)*, at 50-51(Jan. 2006), https://www.ntia.doc.gov/files/ntia/publications/ipv6final.pdf.

- M2M traffic will reach 343.7 Petabytes per month by 2020.
- M2M will account for 11% of total mobile data traffic by 2020, compared to 3% at the end of 2015.
- The average M2M module will generate 612 megabytes of mobile data traffic per month by 2020, up from 192 megabytes per month in 2015.
- The average M2M module (excluding LPWA) will generate 1,081 megabytes of mobile data traffic per month by 2020, up from 207 megabytes per month in 2015.
- M2M modules were 16.89% of device connections in 2015, and 2.82% of total traffic.
- M2M modules will be 54.2% of device connections by 2020, and 10.7% of total traffic.[49]

Currently, most IoT applications operate on unlicensed frequencies, using a range of standards such as Bluetooth, ZigBee, Z-Wave, and Wi-Fi, to name a few.[50] Unlicensed spectrum will continue to play a vital role in the development of the IoT. Ultimately, though, the large amounts of data generated by the IoT will require flexible framework that will make use of both licensed and unlicensed spectrum.[51] While data gathered by sensors may be transmitted short distances over unlicensed spectrum via Bluetooth or the like, that data may ultimately be sent to the cloud via a cellular network. These networks will only become more congested as the number of connected devices increases over time.

[49] Cisco, *VNI Mobile Forecast Highlights, 2015-2020*, http://www.cisco.com/assets/sol/sp/vni/-forecast_highlights_mobile/index.html (last visited May 31, 2016).

[50] Paul Barbagallo, *As 'Internet of Things' Evolves, FCC's Spectrum Strategy Will Be Put to the Test*, BNA: Telecommunications Law Resource Center (Nov. 19, 2014), http://www.bna.com/internet-things-evolves-n17179912070.

[51] *Id.*

5G – the fifth generation of wireless communications technology – is set to become the "backbone" of the IoT, connecting fixed and mobile devices alike.[52] 5G will be a highly flexible and more powerful technology than 4G. It is poised to support specialized IoT applications, including those that have unique technology requirements (*e.g.*, low latency) or business model requirements.[53] As the FCC and the NTIA have recognized, transformation of 4G to 5G requires more commercial spectrum. Cisco endorses NTIA's Assistant Secretary Lawrence Strickling's call for more spectrum, including for 5G,[54] and appreciates that NTIA's Institute for Telecommunications Sciences ("ITS") has begun testing the possible effects of IoT on spectrum usage.[55] It also applauds the FCC for its efforts to identify additional licensed and unlicensed spectrum that can be made available for IoT applications, including its implementation of the 600 MHz "incentive" auction, and for its willingness to explore other creative solutions to spectrum issues in the 5 GHz and "Spectrum Frontiers" rulemaking proceeding focusing on spectrum above 24 GHz.[56] Congress, the NTIA, and the FCC must continue to craft policies that promote creative uses of spectrum, including consideration of how spectrum held by the federal government can be deployed to advance the IoT.

---

[52] Alexander Hellemans, *Why IoT Needs 5G*, IEEE Spectrum (May 20, 2015), http://spectrum.ieee.org/-tech-talk/computing/networks/5g-taking-stock.

[53] Dan Kurschner, *The Cisco 5G White Paper Series*, Cisco Blog (May 9, 2016), http://blogs.cisco.com-/sp/the-cisco-5g-white-paper-series.

[54] News Release, NTIA, *Joint statement following the Biannual Spectrum Planning meeting on Friday, April 1, 2016, between FCC Chairman Tom Wheeler and Assistant Secretary of Commerce for Communications and Information and NTIA Administrator Lawrence E. Strickling* (Apr. 1, 2016), https://www.ntia.doc.gov/speechtestimony/2016/joint-statement-following-biannual-spectrum-planning-meeting-friday-april-1-201.

[55] Request, 81 Fed. Reg. at 19958.

[56] For Cisco's views in these rulemakings, *see* Comments of Cisco Systems, Inc., GN Docket No. 12-268 (filed Jan. 25, 2013); Letter from Mary L. Brown, Senior Director, Government Affairs, Cisco Systems, Inc., to Marlene H. Dortch, Secretary, FCC, ET Docket No. 13-49 (filed Dec. 23, 2015); Reply Comments of Cisco Systems, Inc., ET Docket No. 13-49 (filed July 24, 2013); Comments of Cisco Systems, Inc., ET Docket No. 13-49 (filed May 28, 2013); Comments of Cisco Systems, Inc., GN Docket No. 14-177 et al. (filed Jan. 28, 2016).

iv. Ensuring Security of Systems

The Request correctly recognizes that a "growing dependence" on embedded devices raises significant privacy and security concerns.[57] In order for the IoT to reach its full potential, customers and end users must trust that their data is being securely transmitted. M2M networks potentially open up new vectors for attack that need to be managed thoughtfully. As the Federal Trade Commission ("FTC") has rightly pointed out, a well-designed and secure network is fundamental to protecting the vitality of the IoT.[58] This is an area where significant challenges and opportunities for improvement remain. With low barriers to entry, new entrants that lack sophistication or expertise may be unfamiliar with best practices for technology or may not prioritize security, developing poorly designed, vulnerable hardware or software. Low-cost new devices and legacy devices without connectivity capabilities may lack update mechanisms, unable to get critical and much needed security updates and patches. Companies that are new to the development of network-connected technologies (like auto manufacturers) will be exposed to new threats, and may initially react to the discovery of vulnerabilities with threats of litigation or even criminal prosecution, which may chill research and efforts to identify and fix security flaws.[59]

Subjecting the IoT to a separate regulatory regime, however, is not the appropriate response to these challenges. Prescriptive regulatory approaches are generally not capable of

[57] Request, 81 Fed. Reg. at 19959.

[58] FTC, Staff Report, *Internet of Things: Privacy & Security in a Connected World*, at 55 (Jan. 2015) ("FTC Staff Report"), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[59] Katie Bo Williams, *Fear of lawsuits chills car hack research*, The Hill (Oct. 3, 2015), http://thehill.com/policy/cybersecurity/255832-fear-of-lawsuits-chills-car-hack-research. NTIA's efforts to promote responsible norms of behavior around coordinated vulnerability disclosure are useful and should continue to foster a mature dialogue aimed at promoting important security research.

adaptation to dynamic threat environment and at the same time limit the ability to innovate.[60] Instead, governments should work within the context of existing regulatory structures, focusing on outcome-oriented approaches for managing newly identified risks associated with the use of particular technologies as opposed to regulating the underlying technologies themselves. Government should also look to reduce conflicts between existing industry verticals and improve cybersecurity risk management through effective multi-stakeholder, public-private partnerships aimed at development of industry-led, globally-recognized best practices and standards.

When it comes to government policies relating to the management of security risks, Cisco believes there are three key guiding elements: (1) solutions to security threats must be global in nature; (2) approaches to security must remain flexible and leverage consensus-based standards; and (3) total security is neither possible, nor given the costs, desirable. Where security obligations are imposed, they must be flexible enough for a dynamic threat environment and appropriate to the risks presented in order to effectively apply available resources. The norms associated with managing security risks are evolving, and sectors are working to find tailored solutions to address their particular needs and circumstances. A standards-based approach to managing cybersecurity risks in partnership between the owners and operators of critical industry and their regulators has the advantage of focusing limited resources on the problems that are most consequential.

Education will also be a key driver to ensuring a strong, secure backbone for the IoT. If industry expects more space and time to be allotted for the IoT market to mature, it must design, develop, maintain, and operate its products and services with security and privacy in mind.[61]

---

[60] *See* FTC Staff Report.

[61] *See* Eric Wenger, *The First Law of IoT: Things that Can Be Connected, Will Be Connected*, Cisco Blog (Feb. 25, 2016), http://blogs.cisco.com/security/the-first-law-of-iot.

Government and industry must work together to promote voluntary best practices (including security testing and risk analysis) and implementation of security by design across the board. The FTC has initiated an excellent program aimed at seeding notions of security by design into the business plans of early-stage startups. The program, called "Start with Security," is based on learnings distilled from FTC security-related enforcement actions. FTC staff has produced practical guidance for businesses and offered live presentations in markets where startups proliferate, like Silicon Valley and Austin. More work should be done to build on this program's success. In addition, the FTC should work closely with the National Institute of Standards and Technology ("NIST"), the Department of Homeland Security, and the Small Business Administration to incorporate notions of security-by-design and privacy-by-design into education materials around the use of Cybersecurity Framework published published for the benefit of small and medium-sized businesses.

v. Data Privacy and Use/Ownership of Data

Alongside security, the other element of customer and end user trust is privacy. The value of the IoT is driven by the data being collected by the connected devices. But that raises questions as to how existing data protection frameworks can be applied in order to enable the IoT to flourish while protecting data in a manner that is appropriate to its use and sensitivity. The IoT implies greater use of data for positive ends, but it also has the potential to leave citizens feeling exposed and/or subject to embarrassment if not handled correctly.[62] It is important that end users know about how their data is used and feel comfortable about it. Organizations are increasingly reliant on effective collection, analysis, use, storage, and management of data for their success. Trust is foundational to any organization that is data-centric, which underscores

[62] Privacy considerations are particularly sensitive with respect to wearable devices that may gather sensitive health data, such as sleep patterns and eating and exercise habits.

the importance of privacy-by-design. While existing notions of data protection *e.g.*, notice and consent remain highly relevant in the context of IoT, it may take some adaption to apply them when devices are too small or low-powered to provide screens or keyboards. Consumer understanding of these technologies and their expectations for appropriate use of their data may continue to evolve as well. In the meantime, a key guide is for those handling customer data to avoid uses of data that are fundamentally out of line with expectations of the data subject and result in embarrassment or surprise.

Notice and Consent. Notice and consent regarding types of data being collected and the nature of its use makes sense from a principled point of view – tell people what you are going to do in the interests of transparency and give them the option to make choices around that. In the IoT world, however, this is not always easy to achieve. M2M devices, such as sensors and actuators, often do not have a user interface, so providing information and check-box options will not always be possible. While we leave space for the technology to adapt, we also need to be aware of what consumers want and expect. The pervasiveness of these devices in the environment could make for a frustrating consumer experience – do we want to be pestered by notices and requests for consent thousands of times as we walk down the street?

In addition, not all data is sensitive – information being collected by agricultural sensors on soil conditions is arguably not as sensitive as data about an individual's health or financial status. The context of how data is being used and who is using it is also important – use of sensors by the airport authorities to implement crowd management may be considered an acceptable use of the data aggregated, but use of those same sensors by an oppressive regime to track the location of its dissidents arguably would not. Similarly, we may be comfortable with medical test results initially collected to diagnose one disease being cross-checked against a rare

disorder down the line, but less comfortable with those same results being sold to an insurance provider without consent.

One alternative solution to the problems with notice and consent is to minimize the collection of personal data. In some circumstances this is fairly straightforward. Sensors collecting soil acidity data are less likely to be seen to be collecting personal data. Others are more complex, such as when the existence of a device owned by an individual is registered but care is taken to ensure that there are no means to identify the individual, for example, by avoiding the collection of identifiers or other factors specific to a person. The ability to conduct processing of data that has been anonymized or pseudonymized will be central to the success of the IoT.

International Considerations. There are also cross-border challenges with respect to privacy. NTIA recognizes that the U.S. is not acting in isolation in this space and must coordinate with its international partners. The EU in particular is known for its horizontal approach to data protections—as contrasted with the US approach built around specific verticals involving highly sensitive data. An inconsistent patchwork of global regulations relating to data sovereignty will undoubtedly impede innovation. We need to make sure that we have usable mechanisms for handling international data transfers and for addressing issues relating to data sovereignty that do not put companies in the impossible situation of being required to comply with conflicting jurisdictional elements. If "harmonization" of data protection requirements is not realistic, we at least need to work towards ensuring that laws, regulations, and policies are interoperable across borders.

Other Big Data Considerations. Big data is a relatively new phenomenon. While government regulators must be mindful of privacy considerations, it is also important to

acknowledge that the greatest benefits from the IoT are derived from the analysis and flow of big data. Overly restrictive application of intellectual property laws could impede the progress of the IoT. To avoid misuse of data, industry should work together to set up frameworks to ensure that contractual provisions clearly spell out issues relating to the ownership and use of data. Public sector data should be open, accessible for reuse, redistribution, and universal participation whenever possible. It must be available as a whole, at a reasonable reproduction cost, and in a convenient form. It should be open to all to use and distribute with no limits on particular purposes or restrictions on commercial use.

vi. Addressing Liability Concerns

With new technology comes new potential for liability.[63] There is uncertainty regarding who should bear the liability for any system vulnerabilities or defects, including inaccurate data. The potential costs associated with potential products liability litigation may discourage the deployment of new IoT technologies.[64] This does not mean, however, that federal or state governments should rush to enact a regime of IoT-specific liability statutes. In the context of assessing liability related to connected cars, The Brookings Institution has noted that traditional products liability law is a "time-tested framework that has proven to be adaptive to technology-driven liability issues in many other contexts" and "subject to a few narrow exceptions, existing tort and contract law frameworks are generally very well equipped" to handle liability issues

[63] Consumer Technology Association & AIG, *The Internet of Things: Evolution or Revolution?*, at 17-18, https://www-160.aig.com/content/dam/aig-mktg/america-canada/us/documents/landing-pages/disruptive-tech/iot/aigiot-english-report.pdf.

[64] Dorothy J. Glancy, *Sharing the Road: Smart Transportation Infrastructure*, 41 Fordham Urb. L.J. 1617, 1645 (Oct. 2014) (noting the delay in the advancement of autonomous vehicles due to fear of costs related to products liability litigation) (citing U.S. Gov't Accountability Office, Gao-14-13, *Intelligent Transportation Systems: Vehicle-to-Vehicle Technologies Expected To Offer Safety Benefits, But a Variety of Deployment Challenges Exist* (2013)).

relating to connected cars.[65] While it is today unclear whether reliance on traditional products liability law will discourage widespread IoT deployment, the issue is one that government should closely monitor, particularly with respect to innovations like autonomous transportation, where there may be unique liability concerns.

vii. Educating, Training, and Preparing the Workforce for the IoT

Workforce education is a particularly pressing need, given the quickly evolving technological landscape. While IoT technologies are evolving at a rapid pace, there is a growing skills gap, creating a need for individuals who understand interactions among IT, networking and traditional control systems. World Bank studies estimate that 200,000 new engineers are required every year from 2014 to 2022 to connect the unconnected.[66] The need for workers skilled in cybersecurity is particularly acute. Workers will require new skills to deploy the IoT infrastructure, be it in design, installation or implementation.

Cisco is leading the charge in educating the workforce for the digital economy by offering online courses and career building programs that are IoT-centric.[67] For example, Networking Academies is a public-private partnership in which Cisco provides free curricula, virtual learning tools, instructional support, teacher training, and professional development opportunities for instructors to millions of students who earn Cisco technical certifications. Cisco likewise participates in numerous mentoring activities, including hosting a *Girls in ICT*

---

[65] John Villasenor, *Products Liability and Driverless Cars: Issues and Guiding Principles for Legislation*, Brookings (Apr. 24, 2014), http://www.brookings.edu/research/papers/2014/04/products-liability-driverless-cars-villasenor.

[66] Press Release, Cisco, *Cisco Introduces New Cloud and IoT Certifications to Address Key IoE Skills* (May 27, 2015), https://newsroom.cisco.com/press-release-content?articleId=1644181.

[67] *See, e.g.*, Cisco, Cisco Networking Academy, *Introduction to the Internet of Everything*, https://www.netacad.com/courses/intro-internet-of-everything/ (last visited May 31, 2016).

Day, job shadow days, a Social Innovation Challenge, and a STEM Day of Action, to name a few.[68]

Cisco is very focused on addressing workforce development, but it cannot stand alone in its efforts to educate tomorrow's workforce. It is critical for the government to play an active role in providing training and educational opportunities to IT and networking professionals to advance skill sets needed for the deployment of IoT technologies. It can accomplish this goal in a number of ways, including partnering with universities to develop cybersecurity and IoT-centric curricula, offering training opportunities to businesses, such as seminars and workshops, and by creating grant and/or scholarship programs focused on STEM education. One thing is certain – if the U.S. wants to be the driver of the IoT technologies, it must prioritize and allocate significant resources to STEM education.

III. CONCLUSION

The IoT is generating unprecedented opportunities for all of us – in the way we govern and are governed, the way we do business, and the way we manage our lives. We stand at the cusp of an era in which everything from cars to cows can be given an Internet address and connected to the IoT network.

The extent of the IoT's success largely depends on getting the technological and policy mix just right. Just as the Internet of the 1990s flourished as the result of a light regulatory touch, so, too, should the IoT.[69] The dynamic threat environment requires a focus on flexible,

---

[68] *See* Cisco, Corporate Social Responsibility, *STEM @ Cisco: Cultivating STEM education and careers needed to build tomorrow's workforce*, http://csr.cisco.com/pages/stem-at-cisco (last visited May 31, 2016). Cisco is also a sponsor of Million Women Mentors, https://www.millionwomenmentors.org/, and the Grace Hopper Celebration for Women in Computing, http://ghc.anitaborg.org/.

[69] *See, e.g.*, Executive Office of the President of the United States, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, 23 (Feb. 2012), https://www.whitehouse.gov/sites/default/files/privacy-final.pdf (underscoring

globally-recognized standards developed through public-private partnerships. In some instances, of course, government action is needed and welcomed. Government can and should encourage industry efforts towards adoption of technology neutral, voluntary, consensus-based, open global standards for IoT. It should assure that patent issues not deter the development of IoT. The FCC must ensure there is an adequate unlicensed and licensed spectrum to support the IoT. The federal government must consult and coordinate internationally to ensure that trade barriers support the free flow of IoT solutions and to assure that data can flow freely across borders through consistent approaches to security and privacy issues. Government can also effectively promote adoption of IoT by investing to bring its cities, infrastructure, military and federal workforce into the digital connected age, encouraging the move to IPv6, and raising awareness of workforce training opportunities. More generally, government must make sure that the tax code promotes innovation and investment, that our education system equips future workers with the capabilities they need to participate in a world where the IoT is a reality, and that our immigration policies support the proper acquisition of talent to maintain the United States' leadership role in the development of the IoT.

Generally, however, the government should exercise regulatory restraint to the greatest extent possible, to avoid the risk of chilling innovation with heavy-handed, inconsistent, or unnecessary regulations. Industry stakeholders must be given room to collaborate and reach consensus on critical issues such as privacy and cybersecurity best practices. Industry is deeply engaged and working cooperatively to address the many technical and policy challenges facing the deployment of the IoT. It can do so with the speed, agility and flexibility that government simply cannot offer. While the government can continue to play a critical role to ensure that its

---

that the Internet is an "open, decentralized, user-driven platform for communication, innovation, and economic growth," and attributing its success to reliance on multistakeholder processes).

policies generally create an environment that promotes IoT innovation, it should continue to exercise restraint and caution, proceeding only when industry calls for it or the government is otherwise uniquely positioned to take action (such as with spectrum management). To the extent government intervention is proposed, that approach should carefully weigh the costs against any purported benefits from such regulation. And finally, as with any regulation, the government must consider any unintended consequences and carefully avoid creating any uncertainty in the marketplace.

There are challenges to the adoption of the IoT, to be sure, but they are not insurmountable. If we get it right, the IoT will provide the platform that will span and nurture the next generation of disruptive and creative innovation, injecting trillions of dollars into our economy and improving our lives in ways that we have yet to imagine.

Respectfully submitted,

Cisco Systems, Inc.

By: /s/ *Mary L. Brown*
Senior Director
Government Affairs

By: /s/ *Eric Wenger*
Director
Cybersecurity and Privacy Policy

Cisco Systems, Inc.
601 Pennsylvania Ave., NW
North Bldg., Suite 900
Washington, DC 20004

June 2, 2016