Before the
DEPARTMENT OF COMMERCE
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION

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

VERIZON'S COMMENTS

Donna M. Epps
Katharine R. Saunders
Melissa Glidden Tye

Verizon
1300 I Street NW
Washington, DC 20005
(202) 515-2459

June 2, 2016

Table of Contents

Before the
DEPARTMENT OF COMMERCE
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION

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

VERIZON'S COMMENTS

I. Executive Summary

The Internet of Things ("IoT") is an expansive, quickly evolving group of products and services that together will transform opportunities for consumers and create new markets for competition. As a leading provider of communications, information and entertainment products and services, Verizon has played a critical role in IoT since its inception. Millions of IoT devices operate on our network. We are working side-by-side with developers in our innovation labs to create connected apps and devices. We have launched our own utility, transportation, and healthcare solutions through our Smart Cities, Networkfleet, GridWide, hum, and Intelligent Track and Trace products. And our ThingSpace Development platform provides a web-based, open development environment for enterprises to manage, develop, and deploy IoT solutions.

Although our experience with IoT is extensive, no single company – or even country for that matter – can realize the full promise of IoT on its own. While already off to a strong start, the IoT market is expanding rapidly and dramatically. Analysts estimate that the installed base of IoT devices will grow from 9.7 billion in 2014 to more than 30 billion by 2020.[1] The

[1] IDC, *Worldwide Internet of Things Forecast Update: 2015 – 2019* (Feb. 2016).

worldwide IoT market spend is estimated to grow from $591.7 billion in 2014 to $1.3 trillion in 2019 with a compound annual growth rate of 17%.[2]

To support this explosion of IoT devices, a robust and secure underlying communications network must serve as a foundation. That network requires both increased commercial spectrum and development of the underlying core infrastructure. We encourage all stakeholders to work together to ensure that these necessary building blocks for IoT development are available and accessible. To enable sufficient spectrum to power this new wave of connected innovation, private and public sectors must continue to cooperate, not only to develop more ways to effectively share spectrum, but also to provide federal users incentives to free up spectrum for commercial licensed and unlicensed use. As potentially billions of new IoT devices are deployed, they will drive data growth that – combined with the parallel growth in overall data usage by consumer devices – will require new commercial spectrum allocations to accommodate the unprecedented demands for more bandwidth. This includes spectrum necessary to support 5G, since 5G's super-fast speeds and low latency will help facilitate new IoT use cases.

But spectrum is only part of the equation. We also encourage NTIA to take action to support policies that will promote investment in the infrastructure necessary to support IoT. To implement 5G, providers will need to densify their networks by deploying additional small cells throughout their footprints and expanding access to backhaul – the fiber optics that transmit data from the small cell to the core network. Currently, in many locations there are substantial costs and regulatory impediments to doing so. NTIA can assist by advocating policies to encourage removing roadblocks to the deployment of the necessary infrastructure to support 5G. These efforts will help to clear a path for continued development and growth.

[2] *Id.*

In addition to the necessary network foundation, IoT needs a consistent policy framework that accelerates, rather than slows down, its growth. We urge NTIA and the Department of Commerce to work with industry and consumer groups to create principles that will guide policymakers on ways to encourage rapid development and deployment in this space. Rather than govern IoT piecemeal, government should harmonize existing regulatory structures. Policymakers should resist the urge to create IoT-specific regulations. Of course, some specific matters germane to a particular industry may require unique regulatory solutions, but in matters that cross all IoT devices, such as privacy and cybersecurity, we should encourage the development of holistic, consistent international and domestic policies that are neutral across industries. Domestically, NTIA should help guide agencies to minimize duplicative oversight or conflicting restrictions. And internationally, entities should work to minimize efforts to impose parochial restrictions on the introduction and movement of IoT devices and products.

Given the breadth and depth of the IoT opportunity, the U.S. government needs to promote a global sense of collaboration, experimentation, and openness to deliver the full benefits of this rapid IoT expansion. Together, we will create cleaner cities, deliver better healthcare, make transportation systems safer, conserve water, boost productivity, and make the digital world work better for everyone. We applaud NTIA's efforts to promote sound policies that will allow a competitive IoT ecosystem to flourish, while at the same time protecting consumers, and look forward to working with the Department of Commerce, NTIA, and other stakeholders as the evolution of our networks paves the way for the IoT revolution.

II. The Internet of Things Is a Global Category of Devices and Services That Together Offer the Promise of New Benefits to Consumers and Increased Opportunities for Competition

A. Given the Rapid Changes in this Space, the Definition of Internet of Things Should Remain Flexible

In these early days of IoT, there is no need to rigidly define "Internet of Things" and risk constraining its development. The term "Internet of Things" is a flexible, developing identifier for a category of products and services that together offer customers new ways of connecting and new opportunities for communications. Absent a firm definition, however, there are general guidelines that should frame the way we think about IoT. IoT is a "broad umbrella term that seeks to describe the connection of physical objects, infrastructure, and environments to various identifiers, sensors, networks, and/or computing capability."[3] In general terms, the term "IoT" refers to "'things' such as devices or sensors – other than computers, smartphones, or tablets – that connect, communicate or transmit information with or between each other through the Internet."[4] The field generally is agreed to encompass "applications and analytic capabilities driven by getting data from, and sending instructions to, newly-digitized devices and components,"[5] and "often enabling the exchange of data across multiple industry sectors."[6]

While these definitions may vary, they all agree on one critical point: IoT devices are fundamentally different from consumer-focused devices such as computers, smartphones, or

[3] NTIA Notice at 3.
[4] FTC Staff Report, *The Internet of Things: Privacy and Security in a Networked World* (Jan. 2015) p. 6 (*available at* https://www.ftc.gov/system/files/documents/reports/federaltrade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf) (2015 FTC Internet of Things Report)).
[5] NTIA Notice at 3.
[6] Ofcom, *Promoting investment and innovation in the Internet of Things* (July 23, 2014) p. 3 (*available at* http://stakeholders.ofcom.org.uk/binaries/consultations/iot/summary/iot-cfi.pdf).

tablets.[7] IoT devices "focus on how computers, sensors, and objects interact with one another and process data."[8] Indeed, a precursor to the term "IoT" was "machine to machine," or "M2M," which referenced the lack of human intervention in communication between devices. Today, most IoT devices use a business-to-business ("B2B") model or a variation thereof. Unlike typical consumer communications devices, the primary purpose of IoT devices is typically to use mobile or fixed connectivity to deliver value-added functionality. IoT services also often have a closed user group, and a limited range of functions. Many of these functions are designed into the service or device itself; the user cannot modify the connection or access different services. These devices are often cheaper, low-power devices with a single or limited use case, and unlike consumer-facing devices, they usually do not have access to personally identifying information.

Thus, any definition of the space needs to be both flexible enough to encompass the wide range of IoT services and devices, but still sufficiently narrow as to distinguish IoT from traditional telecom services, and to divide the IoT landscape into consumer versus industrial or enterprise applications. Regulators should not apply traditional utilities-style telecommunications rules designed to protect end-users to enterprise IoT services. An enterprise device that does not collect personal information does not need the same type of notice and choice mechanisms that might apply to consumer-facing IoT solutions. Devices that communicate solely B2B do not require guidelines for accessibility or access to emergency services.

---

[7] *2015 FTC Internet of Things Report* at 5 (stating that "the 'things' in IoT generally do not include desktop or laptop computers and their close analogs, such as smartphones and tablets, although these devices are often employed to control or communicate with other 'things.'").

[8] *2015 FTC Internet of Things Report* at 5 (quoting Ctr. for Democracy & Tech., #484: FTC Seeks Input on Privacy and Security Implications of the Internet of Things; Comm'n Staff to Conduct Workshop on Nov. 21, 2013 in Washington, DC (June 1, 2013) (*available at* https://www.ftc.gov/sites/default/files/documents/public_comments/2013/07/00028-86211.pdf)).

B. IoT Solutions Present New Opportunities in Multiple Industries

Despite – or because of – the lack of a strict regulatory scheme rigidly defining and overseeing this space, providers are rapidly creating and deploying new applications for IoT. These include innovations in agriculture, healthcare, connected cars, smart cities, energy, and supply chain management. Verizon itself is an active leader in the IoT revolution, not only building the network over which IoT runs, but also as a developer of IoT products and services.

1. Agriculture

As global demand for food increases by approximately 70% by 2050,[9] IoT offers new solutions to help farmers contend with water shortages, escalating costs, and the limited availability of land. IoT "precision agriculture" systems deploy wireless sensors and weather stations to gather real-time data about crops, including soil conditions, moisture, wind, and more. With site-specific data, growers can then optimize growing conditions and improve yields on a plot-by-plot basis, boosting yields, improving quality, and cutting costs in the process.

Verizon's agriculture IoT solution provides just this sort of insight and actionable intelligence to growers. With Verizon technology, Hahn Family Wines uses sensor data and analytics to conserve resources by adding precision to watering and fertilizing at the company's 1,000-acre California vineyard. An IoT gateway continuously monitors data from the various sensors in the vineyard and transmits it wirelessly to Verizon. Using Verizon's ThingSpace dashboard, Hahn can use this data to time and target its use of fungicide sprays to prevent disease and rotting, and can assess the need for watering, fertilizer, or other interventions.

2. Connected Cars

Many of the technology, data, and integration advancements in the IoT field come together in increasingly connected and cognizant cars. A "connected car" is "a vehicle able to

[9] Population Institute, *FAO Says Food Production Must Rise by 70%* (2009).

optimize its own operation and maintenance as well as the convenience and comfort of passengers using onboard sensors and Internet connectivity."[10] Connected vehicle features can include networked entertainment options, real-time weather and traffic updates, detailed diagnostics and maintenance information, navigation and tracking systems, and much more. By 2020, there could be a quarter billion connected vehicles on the road, enabling new in-vehicle services and automated driving capabilities."[11]

Verizon's hum product includes a device that plugs into a car's on-board diagnostic port and gives vehicle owners access to services including boundary and speed alerts, vehicle location, and driving history. Subscribers receive pinpoint roadside and emergency assistance; those with a car problem can talk to a live mechanic via hum's mechanics hotline. Consumers can also get information that allows them to assess estimated pricing on repairs or comparison shop on vehicle parts or accessories.

Telematics technology also has significant application in commercial fleet management, helping fleet operators comply with regulations requiring them to track driving behavior and hours. Our product, Verizon Networkfleet, enables companies to track, monitor, and manage their fleets efficiently and effectively through features such as onboard vehicle diagnostics, GPS tracking, and roadside assistance.

3. **Healthcare**

IoT offers many healthcare solutions including patient monitoring and remote assessment tools. These solutions allow physicians to monitor patients' ongoing conditions remotely,

---

[10] McKinsey & Company, *What's Driving the Connected Car* (Sept. 2014) (*available at* http://www.mckinsey.com/industries/automotive-and-assembly/our-insights/whats-driving-the-connected-car).

[11] Press Release, Gartner, *Gartner Says By 2020, a Quarter Billion Connected Vehicles Will Enable New In-Vehicle Services and Automated Driving Capabilities* (Jan. 26, 2015) (*available at* http://www.gartner.com/newsroom/id/2970017).

without requiring time-consuming in-person testing or visits. Verizon has partnered with AMC Health on a mobile patient monitoring solution, with which a pregnant woman can track blood sugar via a mobile device and communicate readings from the glucometer anytime and anywhere she chooses. With that information stored securely in the cloud, the patient's care provider has timely access to her test results and can better monitor risk to her or her baby.

4. **Energy**

As energy and utility companies work to modernize their infrastructures and comply with ongoing regulatory restrictions, IoT systems are already playing a key role in facilitating quick reactions to emerging issues. New low-power, low-cost grid sensors connected by IoT can immediately analyze a utility's grid and network, reducing cost, improving efficiency, and locating potential troubles. For example, sensors can enable electricity providers to identify potential environmental events like trees interfering with power lines, and schedule foliage maintenance before an accident occurs. Similarly, sensors can monitor voltage, allowing power providers to determine whether a transformer is running too hot, or assess if there is a spike in demand that might require a quick response to optimize the grid. Verizon's own GridWide Utility solution enables utilities to modernize aging infrastructure, increase efficiency, and better control costs by integrating technologies such as smart metering, demand response, and distribution monitoring and control.

5. **Smart Cities**

The world's population is migrating to cities. Fifty-four percent of the world's people live in urban areas[12] and the World Health Organization estimates that by 2050, more than two-

[12] Michael Collyer, *"Three million people move to cities every week": so how can cities plan for migrants?*, CITYMETRIC (Dec. 2015)(*available at* http://www.citymetric.com/skylines/three-million-people-move-cities-every-week-so-how-can-cities-plan-migrants-1546)..

thirds of the global population will be city dwellers.[13] This rapid urbanization is putting a strain on city services as well as on the aging infrastructure including public transportation, lighting, sewer, and sanitation systems.

IoT technology provides a way forward by pairing next generation sensors with advanced analytics to monitor and track data, allowing cities to better understand and plan for growth, increase efficiency, and assist residents. Smart streetlights equipped with motion sensors save cities energy and money because lights brighten and dim when they sense movement. Monitors can identify open parking spaces and direct drivers to them, or can help track and provision cars from car-sharing services to reduce traffic overall. Technology can aid public safety by detecting gunfire in troubled areas, and, with real-time data analysis, pinpoint the location of shots, and notify emergency dispatchers to send police officers to the area.[14]

The Department of Transportation has already taken steps to encourage smart city adoption through the Smart Cities Challenge, pledging up to $40 million to the winning city to integrate innovative IoT technologies into its transportation network. This program is a great way for the federal government to express its support for IoT and smart cities, and to establish a prototype showcasing the benefits of smart city technology. Verizon has launched its own Smart Cities partnership with the city of Boston, part of a much broader effort to transform the city's communications facilities to a new fiber-based platform. The Smart Cities project will help address traffic safety and congestion, as well as future efforts aimed at environmental concerns, energy efficiency, and lighting.

---

[13] World Health Organization, *The Dawn of an Urban World*, Hidden Cities: Unmasking and Overcoming Health Inequities in Urban Settings. The WHO Centre for Health Development, Kobe, and United Nations Human Settlements Programme (UN-HABITAT) (2010), at p. 4.

Car sharing programs will reduce car ownership rates, ensuring more efficient use of vehicles in crowded urban areas. Verizon is partnering with Innova UEV on a university campus-based pilot car sharing program with Innova's all-electric Dash vehicles. The Innova EV Car Share app powered by Verizon enables users to locate, reserve, access, utilize, and then return a shared car, using their smartphone or tablet. It also displays how much carbon emissions are avoided for each ride. This type of program would enable wider use of shared cars, reducing traffic, alleviating parking congestion, and lowering emissions in otherwise crowded areas.

6. **Supply Chain Management**

IoT technology can also help companies reimagine their supply chains. Consider the massive number of touch points in the pharmaceutical supply chain, from plant materials to packaged products on a store shelf. Today, companies use RFID technology to track the movement of products, which is limited to identifying when and where an item is scanned. But IoT solutions, such as Verizon's Intelligent Track and Trace, will provide a more efficient solution to tracking prescription drugs in the supply chain. Other companies will be able to use these products to identify inefficiencies or delays in their shipping and to confirm product integrity from plant to retail sale.

III. Challenges that Could Impede the Robust Development of IoT

As IoT expands, so do the potential challenges to its continued growth. These challenges include cultivating a foundational ecosystem upon which IoT can flourish. A successful IoT environment will need sufficient radio frequency spectrum and robust communications infrastructure; consistent legal and regulatory frameworks that are not overly prescriptive; protection from foreign mandates that create an inconsistent international regulatory landscape; and sustained consumer confidence. The Department of Commerce can play a key role in the

growth of IoT by using its considerable influence and broad stage to advocate policies, both domestic and international, that promote IoT growth.

A. Ensuring Adequate Spectrum and Communications Infrastructure

1. Spectrum

Communications networks, both wired and wireless, are the backbone of IoT. For IoT to flourish, we must ensure that those networks are robust and capable of handling consumer and enterprise demands. The combined growth of IoT solutions and data-hungry services like streaming video are causing an exponential increase in the demands placed on wireless networks. As CTIA recently noted, Americans used almost 137% more data in 2015 than in 2014, share more than 4 million photo, video, and text messages per minute, and stream data equivalent to 59,000 videos every minute.[15] The trend shows no signs of stopping: by the end of the decade, wireless data use in the U.S. "is projected to increase another six-fold."[16] Although technological advancements such as small cells, 4G LTE, and soon, 5G, allow more efficient use of spectrum, these innovations often lead to additional growth in demand, which in turn places immense pressure on the need for more spectrum.

The Department of Commerce and NTIA in particular, should continue their leadership in providing more spectrum for commercial use. NTIA has worked closely with Congress, the FCC, and other government agencies to make significant progress on President Obama's 2010 commitment to make a total of 500 MHz of spectrum available for commercial use by 2020.[17] Each year since President Obama made this commitment, NTIA has published an extensive

---

[15] CITA, Annual Wireless Industry Survey, video, http://www.ctia.org/your-wireless-life/how-wireless-works/annual-wireless-industry-survey (last viewed May 25, 2016).
[16] CTIA, Enabling the Wireless Networks of Tomorrow: Rules of the Road for Pole Attachments in States Across America (April 2016) p. 3.
[17] The White House, Presidential Memorandum: Unleashing the Wireless Broadband Revolution (June 2010) (*available at* https://www.whitehouse.gov/the-press-office/presidential-memorandum-unleashing-wireless-broadband-revolution).

report analyzing potential bands for clearing or sharing.[18] It also has worked closely with federal agencies and the private sector to translate the potential contained in these reports to reality.

Last year's tremendously successful AWS-3 auction was the result of significant public-private cooperation, much of which was done under the auspices of the Commerce Spectrum Management Advisory Committee (CSMAC), which NTIA leads. These efforts resulted in an auction of 90 MHz of prime spectrum, 45 MHz of which previously was exclusively allocated for federal spectrum. Now that spectrum is licensed for commercial use, and still shared, in part, with some federal users. NTIA also has worked closely with the FCC to ensure that commercial users can effectively share spectrum with government users, most recently with the novel database and sensing approach to commercial users sharing with naval radars in the 3.5 GHz band. This work is critically important, not only to free up the 3.5 GHz spectrum, but also to test the sharing mechanisms developed for potential use in other bands.

Verizon has supported many of NTIA's efforts to-date. And we will continue to work together to ensure that there is sufficient spectrum to power this new wave of connected innovation. We will continue to help NTIA advance efforts to share government and commercial spectrum. But we believe it is also necessary to find more spectrum for commercial licensed and unlicensed use. NTIA should continue its work with federal agencies to relocate systems as quickly as feasible from AWS-3 uplink spectrum that is licensed, but not yet cleared, for commercial mobile broadband. Also, as it has each year since 2010, NTIA should continue to cooperate with federal agencies to identify new bands that may be repurposed for mobile broadband. NTIA and other federal agencies have worked closely with Congress to implement a CSMAC recommendation to provide additional resources to federal agencies in order to identify

[18] *See,* NTIA, 500 MHz Initiative, U.S. Department of Commerce (*available at* https://www.ntia.doc.gov/category/500-mhz-initiative).

such candidate bands.[19] NTIA should take those efforts a step further and encourage Congress to enact legislation that would offer additional incentives to agencies to improve their spectral efficiency, and potentially free up more spectrum for commercial use.[20] Last, the Department should urge Congress and the FCC to strike a reasonable balance between licensed and unlicensed spectrum when allocating new commercial spectrum.

2. **Infrastructure**

In addition to encouraging federal stakeholders to make more spectrum available, the Department can help promote policies that ensure efficient deployment of the infrastructure necessary to support use of that spectrum. The next technological revolution in wireless connectivity is 5G, which requires a dense network of small cell receivers. 5G has massive potential to meet increasing wireless demands, including those that IoT will bring. With speeds measured in multiple gigabits per/second, latency in the single milliseconds and the capacity to handle 1,000 times more consumption than current network technologies, 5G promises to deliver on IoT opportunities like robotics, autonomous vehicles, and the massive scale expected in a truly connected world. But its success relies on having the right infrastructure in place, and its timely success relies on deploying that infrastructure without delay.

As discussed above, Verizon has recently launched a partnership with the city of Boston to transform the city's communications network to a new fiber-based platform, as well as improve wireless services by building out the small cell architecture. This three-year, $300 million project will make Boston one of the most technologically advanced cities in the country, offering enormous bandwidth and speeds and providing the robust communications network

[19] *See* Bipartisan Budget Act of 2015, Spectrum Pipeline of 2015, H.R. 1314, 114th Cong. (2015).
[20] As contemplated in bipartisan and bicameral legislation introduced by Representatives Matsui and Guthrie and Senators Fisher and Markey. *See* Federal Spectrum Incentive Act of 2015, H.R. 1641, 114th Cong. (2015); S. 887, 114th Cong. (2015).

foundation necessary to support technological innovations, including IoT. Boston's leadership and commitment to support the necessary infrastructure is – and will continue to be – critical. Boston streamlined their permitting processes to facilitate expeditious implementation of a robust fiber infrastructure, enabling small cell densification and other advanced services to the city. NTIA should urge other cities to undertake similar cooperative endeavors to encourage the deployment of new infrastructure in their own cities. Doing so will allow even more Americans to enjoy the benefits of next generation networks and IoT.

NTIA and others can help promote policies that encourage deployment of small cells. In order to meet burgeoning demand, wireless networks increasingly integrate smaller antenna technologies such as distributed antenna systems and small cells. These facilities are placed on towers, buildings, poles, and other increasingly diverse locations. The federal government should lead by example by expediting tower and small cell siting on federal lands. NTIA's Broadband Opportunity Council has made several recent recommendations and timelines to help infrastructure siting, which are a good step in the right direction. NTIA should also help educate local policymakers on the benefits of IoT and how creating an environment that makes it easier for companies to upgrade their networks will accelerate the benefits that IoT solutions will deliver to their citizens. NTIA can encourage states and municipalities to facilitate 5G build-out by amending state and local laws and adopting best practices to modernize and streamline outdated right-of-way requirements, ensure nondiscriminatory access to local infrastructure like poles and buildings, create just and reasonable rates, and adopt efficient permitting processes.

Finally, wireline backhaul (primarily fiber) is necessary to carry all of this wireless traffic. NTIA should encourage Congress, the FCC, and other federal stakeholders to promote competition by removing obstacles to the deployment of fiber. For example, Congress or the

states can adopt "Dig Once" provisions requiring municipalities to install broadband conduits during street construction projects. More generally, NTIA should promote policies domestically and abroad that would make it easier for network providers to invest in and build out the robust, secure networks that will enable IoT solutions.

B. The U.S. Should Apply Consistent and Reasonable Legal and Regulatory Frameworks to the Internet of Things

The U.S. should have a consistent and strategic approach to IoT-related policy matters. Although U.S. agencies have so far avoided major problems in this area, federal regulators have been active in developing position statements or guidance[21] that threaten a piecemeal approach to policy development for IoT related matters. Inconsistent and duplicative policies will only undermine the growth of IoT as providers try to navigate a sea of conflicting rules. NTIA can play a constructive role to prevent the proliferation of ad hoc rules by laying out an affirmative IoT strategy and guiding principles that other government agencies should follow when thinking about the best policy approaches to promote, rather than hamper, IoT. NTIA could also lead an intra-agency taskforce to ensure better coordination and alignment among federal agencies on IoT related policy issues.

There are a few foundational principles NTIA should consider. First, policymakers should avoid adopting sweeping new regulations to govern IoT solutions. While IoT has the potential to revolutionize the way business is done, it is still simply an extension of existing network and device technology. As a result, many sound frameworks are already in place to address most of the policy issues relating to IoT. Existing policies and policy frameworks should

[21] *See, e.g.* FDA, *Postmarket Management of Cybersecurity in Medical Devices: Draft Guidance for Industry and Food & Drug Administration Staff* (Jan. 22, 2016) (providing agency recommendations for monitoring, identifying, and addressing cybersecurity vulnerabilities in medical devices after they enter the market); 2015 FTC Internet of Things Report (urging companies to take steps to enhance and protect consumers' privacy and security in the context of IoT); FCC TAC IoT Working Group Position Statements (Sept. 23, 2014) (containing statements on IoT issues such as privacy and device end-of-life).

serve as the starting point when considering policy in the IoT context, rather than adoption of new IoT-specific regulation.

Second, the United States should take a uniform and holistic approach to developing policies on those macro issues, such as privacy and cybersecurity, which cut across all types of IoT solutions, regardless of industry segment. For these issues, we should not reinvent the wheel: the principles and processes that are in place today to guide policy development regarding privacy and cybersecurity are sufficient to frame the right approach in the IoT context.

Third, given the breadth of industry segments that IoT devices touch, some IoT solutions may create issues that require a particular agency's sector-specific expertise. But in those limited instances, agencies should only address those specific issues that are unique to their particular sector (such as healthcare, agriculture, aviation), rather than adopting broad new IoT frameworks to tackle macro issues that are common across all IoT solutions. When regulating in their areas of expertise, individual agencies should make sure their policies are narrowly-tailored to the sector-specific issue and refrain from taking actions that could disrupt the broader IoT ecosystem or create conflicts that could impede IoT deployment. Overly prescriptive mandates that dictate particular equipment, programming, or technology that IoT providers must use risk undermining competition and precluding the introduction of innovative new services.

Fourth, policymakers need to acknowledge the key differences between consumer and industrial IoT solutions. Consumer facing IoT devices require a different set of policy considerations than M2M solutions. Many of the traditional consumer protection policies that make sense for consumer facing devices are not applicable for enterprise IoT devices, because the latter are often single-purpose "dumb" technology without access to any customer's personal identifying information. Thus, given the key differences between consumer telephone service

and IoT services and devices, it would be a mistake to apply utilities-style telecommunications or consumer protection laws to IoT.[22] Similarly, policies should be closely calibrated to the type of IoT technology and intelligence of the IoT device. For example, regulations that apply to sophisticated consumer smartphones should not apply to small, low-cost enterprise devices that are best suited for lower tiers of service. Thus, NTIA should oppose both domestic and international efforts to impose outdated telecom regulations on IoT solutions.

Finally, policymakers should adopt a "do no harm" approach to the still nascent IoT market. In the first instance, policymakers should allow room for industry-led, market-based solutions to address emerging new issues. Taking a "wait and see" approach, particularly where there are ongoing industry efforts to address an issue, is the best way for policymakers to avoid premature regulation that could have harmful unintended consequences. Policymakers should step in only if market forces fail to address a persistent issue, but should do so using consensus building models that involve industry input such as multi-stakeholder processes to create principles or best practices rather than resorting immediately to regulation.

1. Existing Privacy Policy Frameworks Provide Appropriate Guidance for Incorporating Privacy Protections into IoT Solutions.

Policymakers should leverage existing privacy frameworks – including the existing FTC regime and self-regulatory mechanism – to create a holistic policy approach to IoT-related privacy issues. Doing so will create the necessary regulatory certainty and stability to support continued investment and growth in IoT solutions.

As a threshold matter, it is important to step back and consider the nature and the type of data that IoT devices generate. Not all IoT devices generate personal data; many IoT devices

[22] For example, as discussed below, the International Telecommunication Union is considering classifying IoT as a traditional "telecommunications service" that the ITU would have jurisdiction over. Such a finding would allow the ITU to regulate roaming, security, privacy, and pricing, and would impede the development of IoT.

designed for business and industrial use facilitate machine-to-machine communication and may not involve the collection of personal information. IoT applications that focus on environmental issues, factories, machines, infrastructure, and energy may not involve data about individuals. Enabling existing industries to better track, manage, and automate their core functions is one of the most promising IoT applications. Many of these industry applications will not implicate privacy concerns as they do not involve personal information. And even where IoT applications do collect personal information, that information is often anonymized to create the large scale data sets needed to identify trends that inform better decision-making.

Although IoT enables the collection of data through inter-connected devices that previously may not have been feasible, the underlying data collection is not a new policy issue that would warrant a new framework for addressing privacy. IoT incorporates technologies that collect a wide variety of data, much of which is already subject to existing laws and self-regulatory mechanisms. The FTC's existing privacy framework, which incorporates many of the Fair Information Practice Principles (FIPPs), is well suited to address the IoT environment. The FTC's flexible method of balancing privacy and innovation should serve as the guiding principle for addressing privacy issues in connection with IoT. And the FTC is the best single federal agency to deal with the privacy implications of new IoT solutions uniformly.

NTIA should expressly discourage the development of discrete IoT-specific privacy policy-making or legislative efforts by an array of different federal agencies or states. Creating a patchwork of new IoT-specific privacy regulations and laws for different IoT devices would only result in a confusing policy landscape that will delay IoT deployment and undermine innovation. Moreover, such new regulations and legislation are unnecessary considering that existing privacy

laws already apply in the IoT environment. Instead, the existing FTC privacy framework,[23] built on important concepts such as transparency, privacy by design, consumer choice, and security, provides the necessary roadmap to guide industry to develop, deploy, and maintain IoT solutions in both a privacy-protective and secure manner. This framework is easily adaptable to the Internet of Things. The FTC should also continue to use its enforcement tools and apply its existing policy guidelines in a technology-neutral manner, as it has effectively done so far.

But FTC oversight is only one part of the right strategy to foster responsible deployment of IoT solutions. As IoT continues to evolve, industry guidelines and codes of conduct, including those developed through multi-stakeholder processes, will continue to be extremely important tools in protecting consumer privacy. These types of guidelines and codes of conduct enable organizations to implement best practices as appropriate within their organizations and consistent with their business models. We agree with the Administration's 2012 White House Privacy Report that privacy-focused multi-stakeholder processes can offer solutions in a more expedient manner than regulatory or legislative processes. We urge NTIA to champion that balanced and flexible framework across all IoT solutions.

2. Cybersecurity Concerns Should Be Addressed Through a Collaborative Process

Like privacy, cybersecurity issues cut across multiple fields and industries. Rather than being regulated by individual agencies or overlapping jurisdictions, therefore, NTIA should encourage an industry driven, collaborative approach to development of seamless, technology-agnostic security standards.

In many respects, the IoT environment shares the same security concerns as other networks: application flaws, software or hardware vulnerabilities, improperly configured or

[23] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (March 2012).

patched components, insufficient encryption, etc. But these concerns are amplified by the sheer volume of IoT devices constantly communicating and requiring reliably authenticated access to networks. To ensure a consistent and strong national strategy that protects our connected assets and communities, cybersecurity must be addressed and coordinated on a broad scale across the entire ecosystem, with consistent and complementary efforts.

To address these concerns, we believe that government should follow a path similar to that already created in the NIST Cybersecurity Framework. By adopting an analogous industry-driven, collaborative approach, the relevant stakeholders could identify voluntary standards, guidelines, and practices to protect IoT solutions from cyber risks. Just as the NIST framework was developed through a collaborative process that included industry, academia, and government stakeholders, a similar process for IoT cybersecurity could produce a broad framework that would guide the development of more specific technical standards in an environment that remains flexible, collaborative, and current. These standards should focus on authentication of devices and the security of network connections in the IoT environment. Such a focus would advance consistent protections against the injection of rogue commands, the corruption of critical data, and data leakage. It would also address concerns that compromised IoT devices could give an attacker access to larger communications networks. By developing standards in a collaborative, industry-driven approach, rather than a "top down" or regulatory manner, the industry can better keep pace with ongoing technological development. As new inventions and use cases are developed – and as cybercriminals shift tactics to try to gain advantage – this flexible approach will allow cyber-defenses and strategies to shift to meet them.

Given the proven effectiveness of the voluntary standards approach, it is unsurprising that industry has already started to collaborate in their development. For example, in the industrial

controls sector (which supplies technologies deployed across many other sectors), industry experts are working to draft specific technical standards that build on NIST SP800-82-R2 ("Guide to Industrial Control Systems Security"); these standards, captured in the ISA/IEC 62443 series, will ultimately shape some of the critical technology for the IoT environment. Similarly, there are significant public/private partnerships, some of them global in scale, that are specifically integrating security into their broader IoT standards development work (examples include the work of the Industrial Internet Consortium, the IoTivity Project of the Open Interconnect Consortium, and the 3rd Generation Partnership Project ("3GPP"). There are also sector-specific efforts underway, some of which leverage both Information Sharing and Analysis Centers ("ISACs") and the new Information Sharing and Analysis Organization ("ISAO") authority. Government action should support these efforts, and allow them to fully mature with the growth of the IoT environment.

Further, device manufacturers, application developers, and network providers must develop a "culture of security" and adopt IoT best practices throughout the lifecycle of IoT products and services, whether through rigorous in-house "security by design" practices, or by relying on outside expertise. Through its ICSA Labs division, Verizon launched a new cybersecurity testing program to provide assurance testing for IoT devices and sensors. The program will test devices for weaknesses and certify that vulnerabilities are mitigated as well as test devices over their lifecycle to further improve security. These types of testing programs and certification underscore industry's expertise, interest, and ability to care for cybersecurity.

C. IoT Solutions Will Benefit from Technical Standards To Drive Interoperability, but Industry Standards Bodies Are Making Good Progress

IoT devices must communicate with each other and the network in a seamless and secure manner. The growth of new IoT technologies will thus depend on interoperability, or the ability

to transfer information across systems, applications, or components in four broad layers — technological, data, human, and institutional.[24] As noted by McKinsey, "interoperability is required to unlock more than US$4 trillion per year in potential economic impact for IoT use in 2025, out of a total impact of US$11.1 trillion … . On average, interoperability is necessary to create 40 percent of the potential value that can be generated by the IoT in various settings."[25]

Standards can facilitate interoperability across the IoT ecosystem, foster investment, and increase competition. The good news here is that industry standards bodies are already developing technical standards for IoT. For example, GSMA has begun working to promote interoperability by defining 3GPP standards for IoT devices.

As these processes make progress, there is no need for domestic or international government intervention on technical standards. Instead, government should let the commercial market and industry standards-setting organizations determine the standards that will eventually drive interoperability of IoT devices and networks, and should encourage international regulators to do the same. Appropriate standards can facilitate global interoperability, contribute to economies of scale, and create technical specifications to which innovators can build. Standards should be developed by private sector standards development organizations via inclusive and transparent processes and be available for voluntary use. Appropriate standards should also leave room for variation and the use of proprietary standards and technologies.

In contrast, countries and governments that insist on using a single standard developed or approved by a national government can encourage protectionist behavior that stifles IoT growth. Such country-specific approaches are often designed to benefit national players at the expense of

[24] Philippa Biggs et al., *Harnessing the Internet of Things for Global Development, ITU/Unesco Broadband Commission for Sustainable Development,* p.44 (2016) .
[25] Manyika, James, et. al, *The Internet of Things: Mapping the Value Beyond the Hype, McKinsey Global Institute,* pp. 2, 4 (June 2015).

others, and may be inferior to market-based innovations. Further, they may cause first movers unnecessary delay in IoT deployment by requiring a cumbersome standards development process. Thus, the United States may seek to discourage other governments from proceeding with single, country-specific standards or requiring prior government approval of standards before companies can deploy new parts of the IoT ecosystem.

D. NTIA Should Encourage IoT Global Solutions, Rather Than Country-Specific Regulations

Most IoT devices are fundamentally untethered to geographic boundaries. Sensors transmit data that crosses international borders, is analyzed and re-transmitted, and is managed through global systems and the cloud. A wireless IoT device could be manufactured in Country A, provisioned with a SIM card and shipped from country B, and purchased by a consumer in Country C, who then takes the device to Country D for an extended period. These global use cases – if permitted to develop – could benefit citizens in multiple countries around the world.

But rather than increased flexibility for IoT devices, we are seeing the rise of country-specific measures and national or regional barriers that could fragment IoT. Some countries have implemented specialized M2M and IoT legislation and licensing rules that require country-specific device identifiers, or oblige providers to locate data from IoT devices within a particular country. Other countries have imposed or are considering government mandates relating to privacy and cybersecurity requirements, technical standards and interoperability, and roaming.

NTIA should oppose these requirements, while engaging in various international forums to promote light-touch regulatory approaches that allow the ample flexibility needed for the IoT to flourish. NTIA can also urge governments and inter-governmental organizations to adopt generally applicable policies rather than new technology-specific regulations to the maximum extent possible, and to refrain from applying existing telecom-specific regulations to IoT.

1. Country-Specific Requirements May Create Barriers to IoT Growth

a. Specialized IoT Legislation and Regulations

The International Telecommunication Union (ITU) has recently begun developing IoT-specific requirements that risk conflating IoT services and devices with traditional consumer telecommunications products. The United States should engage in these proceedings to encourage development of polices that recognize the essential differences between enterprise-focused IoT devices and consumer devices used for telecommunications.

The ITU Telecommunications Sector has developed a new group – Study Group 20 – to develop standards and recommended regulations on IoT, and is studying M2M issues in the group responsible for telecommunications rates and tariffs. We understand that other inter-governmental organizations such as the Inter-American Telecommunications Commission (CITEL) and the Asia-Pacific Economic Cooperation (APEC) are considering similar approaches. We are concerned that the ITU may treat IoT services as traditional "telecommunications service" over which the ITU would have jurisdiction. This model could promulgate troubling model rules that would apply telecom-oriented regulations for roaming, security, privacy, and pricing to enterprise M2M and IoT services.

But, as discussed above, imposing outdated regulatory classifications would impede the development of IoT. Most of these devices are enterprise-driven, rather than consumer facing, and much of the regulation that might pertain to smartphones or consumer mobile devices is either inapplicable or actually harmful to the field. We encourage the United States to focus intensively on these trends in the ITU and in other inter-governmental organizations, to discourage this approach, and to encourage policies that will permit the increased growth of IoT.

b. Special Licenses and Other Registration Requirements

We have also seen foreign governments begin to apply special registration requirements to IoT devices. These requirements include obligations that providers obtain a specific license for every device, or register the device's number and IP address. For example, Singapore has established a license for M2M services and a requirement that every device number be registered with the government. Although the government there recently clarified that providers need not provide advance notice before importing a device, the regulation remains in place. India is also considering imposing a registration requirement, and Germany previously considered one.

Given the wide range of current and potential IoT services, such registration requirements, which hearken back to traditional telephony, will limit rather than enable the evolving IoT ecosystem. Device-by-device registration obligations would increase the cost of deploying new IoT services, and discourage providers from expanding deployment to new countries for fear of enforcement action from inadvertent noncompliance. And, these obligations are often not warranted. Reporting and transparency rules designed as consumer protection may not be relevant to business-to-business services and other IoT enterprise arrangements.

c. Device Identifiers

Where traditional telecommunications devices are traditionally identified by their telephone number, IoT devices may use a variety of unique identifiers, including phone numbers, global non-geographic ITU numbers, and IP identifiers, depending on the type of device, the degree to which the device will be mobile, the device use case, and other factors. But despite this variety, a number of countries have begun to consider mandates that IoT devices use only certain types of unique identifiers. Other countries have imposed restrictions on the use of extraterritorial identifiers altogether or do not allow the use of foreign SIMs in certain IoT

devices. And still others limit roaming or seek to impose voice or data roaming restrictions on IoT devices.

Continued adoption of these requirements will erode providers' abilities to deliver consistent global offerings and slow the expansion of IoT. When mandated IoT identifiers are inconsistent between countries, providers will have to create a country-specific version of each device. Devices will be difficult or expensive to use across geographic regions. As a result, providers will face fragmented markets and additional barriers to expansion and entry. NTIA should urge countries and other international actors to refrain from mandating that IoT providers use specific device identifiers. NTIA should similarly oppose efforts by countries or regions to impose voice or data roaming regimes or restrictions on IoT devices. Instead, IoT providers should continue to have maximum flexibility in deciding what identifiers they will rely upon, and to design devices that are able to roam on a variety of networks because different IoT services may have different requirements. NTIA should encourage policies that let commercial agreements – and not government mandates – establish roaming practices for IoT devices.

d. Data Localization Requirements and Other Privacy and Cybersecurity Requirements

As IoT devices exchange and analyze data, they may upload portions of that data to the cloud or to global servers. But a growing number of countries – including, we understand, Australia, China, Brazil, France, Greece, India, Indonesia, Kazakhstan, Malaysia, New Zealand, Nigeria, the Philippines, Russia, South Korea, Taiwan, Turkey, and Vietnam – have proposed or adopted obligations to keep various types of data and locate servers and other computing facilities within their country.

We are concerned that these country-specific data localization requirements impede the cloud computing and data analysis that are central to IoT. While countries may attempt to

characterize localization requirements as privacy and cybersecurity measures, these obligations can impede the free flow of information and data analysis that is necessary to unlocking the full potential of IoT. Data localization requirements can also impose barriers to seamless communication between IoT devices and increase the costs of deploying global solutions.

NTIA and other U.S. government entities have historically promoted seamless cross-border data flows. They should build on this foundation by increasing advocacy for removal of country-specific localization requirements through dialogs with counterparts, international trade norms, global public policy development, exchange of expertise on technology developments, and identification of best practices. They should also encourage reliance on industry-led multi-stakeholder organizations to develop cybersecurity policies as discussed above.

2. The Government Should Engage With International Stakeholders to Promote Policies Favorable to IoT.

The United States should make adoption of favorable IoT policy a top priority in its bilateral and multilateral engagements with other governments and intergovernmental organizations. By advocating for a technology-neutral and market oriented global policy environment for IoT solutions, the U.S. can set a strong example that will help continue to open doors for ongoing IoT growth.

The right time for international engagement is now. International bodies are currently conducting public policy proceedings about IoT, and individual governments are beginning to roll out their own – sometimes conflicting – approaches to regulation. The ITU is considering international standards and rules. The Internet governance community is engaged, with numerous workshops at the annual global Internet Governance Forum discussing cross-border data flows, a seamless global Internet, and approaches to extraterritorial jurisdiction issues. And there are policy bilaterals conducted by NTIA, the new program for Digital Attachés at U.S.

Embassies, formal and informal work around international trade, and technical capacity-building programs such as the U.S. Telecommunications Training Institute.

In this context, the United States is poised to actively participate in the global dialogue on these issues. The Department of Commerce, NTIA, and other government entities should engage closely in international fora and with their counterparts to advocate for policy approaches that will drive a global enabling environment for IoT. The United States can also work to convene international meetings regarding the standards and guidelines for IOT that will encourage diverse stakeholders to come together to develop collaborative solutions.

D. NTIA Can Help Increase Public Acceptance of and Ameliorate Concerns About IoT

NTIA can promote the growth of the IoT by educating the public about the many ways IoT can improve the way we live, work, and play. Today, many consumers and businesses may be nervous about adopting IoT solutions. Consumers may fear that their privacy and data could be compromised or that a hacker could wreak havoc by using IoT to take control of critical infrastructure or connected cars. Customers may have concerns about automated products in their home or business that they do not understand or may not fully be able to control. And businesses may worry about whether an IoT device will adequately respond to new or emergency situations and who bears the liability if an IoT device malfunctions.

These consumer confidence concerns could pose a serious barrier to the growth of the IoT economy. The public may be hesitant to accept IoT solutions, or may be resistant to new devices. But increasing access to information and proactive education campaigns about the benefits of IoT solutions can help address these concerns, as can increased governmental adoption of IoT solutions and use cases. NTIA can help the public understand the basic role that security plays in the design of IoT devices. Because safety is critical, NTIA can launch a public

awareness campaign regarding the importance of IoT devices embedding security protocols at every step of the device's development, including architecture, testing, validation, and deployment. NTIA could convene forums and promote industry-led certification processes that support safety for consumers and businesses.

NTIA could also create forums with stakeholders to explore legislation or regulatory mechanisms governing risk-shifting between consumers and IoT manufacturers. Such an approach could help balance private ownership of devices with accelerated adoption of IoT solutions. NTIA forums or workshops could also address the possibility of policies for insurance coverage relating to IoT devices and harms resulting from their malfunction.

In addition to responding to fears about the IoT economy, NTIA and government can help create a framework to increase public awareness of the benefits of IoT. Just as the Department of Transportation has created its Smart Cities programs, other federal agencies could create similar projects to drive funding for IoT pilot projects that will demonstrate the benefit of these solutions to neighborhoods and citizens. Government can create test beds that deploy new sensors and monitoring for utilities. Schools can include IoT information in curricula, especially STEM programs, or help create internships focused on IoT developers. Government agencies can support public acceptance of IoT by creating grants for programming by third party organizations to create educational programs about ways IoT can improve personal safety, quality of life, and save money for seniors or under-served communities. Government can also explore tax incentives for IoT manufacturing or other related job-creating businesses in lower-income communities or areas. And internationally, the United States can encourage other countries to promote innovation and investment in these new technologies.

As the Internet of Things evolves, it would be useful to have more industry-wide data to chart its progress and inform future decision-making. While the industry is still too young to bear the burden of mandatory reporting requirements, the government could conduct a periodic census that compiles information collected on a voluntary basis from IoT participants. This type of voluntary census could collect information about (1) the types of connections used by IoT devices, such as whether the device connects to a mobile, fixed, cellular, satellite, Wi-Fi, or low-power, or wide-area network; (2) the different types of devices in use; (3) the amount of data and spectrum (if applicable) those devices use; and (4) whether there are meaningful differences across industries and sectors. This type of broadly-sourced data could equip the industry with knowledge to make smarter decisions about the most effective way to deploy future IoT solutions and better serve customers.

Respectfully submitted,

/s/

Donna M. Epps
Katharine R. Saunders
Melissa Glidden Tye
Verizon
1300 I Street NW
Washington, DC 20005
(202) 515-2459