DEPARTMENT OF COMMERCE

National Telecommunications and Information Administration

The Benefits, Challenges, and Potential Roles for the Government In Fostering the Advancement of the Internet of Things

Docket No. 160331306-6306-01

COMMENTS OF AT&T SERVICES, INC.

Robert C. Barber
James Wade
David Lawson
AT&T Services, Inc.
1120 20th Street NW
Suite 800
Washington, D.C. 20036
(202) 457-2121 (phone)

June 2, 2016

Contents

INTRODUCTION AND SUMMARY

AT&T[1] respectfully submits these comments in response to the Department of Commerce ("DOC") and the National Telecommunications and Information Administration's ("NTIA") Notice and Request for Comments on the current technological and policy landscape surrounding the Internet of Things ("IoT"), including the potential benefits and challenges of IoT technologies and the possible roles, if any, that the federal government should play in fostering the advancement of IoT in partnership with the private sector.

NTIA's inquiry is timely because even in its still-nascent stage IoT has established itself as a growth engine throughout the US—and indeed, the global—economy, and its importance will only continue to expand. The IoT is revolutionizing entire industries by allowing Internet-connected machines to communicate directly with other Internet-connected machines, and with cloud computing platforms that analyze data coming off the connected devices, display it across user interfaces, and even provide input and direction back to the connected devices. These machine-to-machine (M2M) communications and the associated analytics platforms, all constituent parts of the IoT, have already demonstrated the potential to greatly improve efficiency, productivity, and social welfare in fields as diverse as education, healthcare, transportation, energy, security and agriculture.

Indeed, IoT technology is finding its way into almost every portion of our daily lives and our nation's economy: smart cities; connected cars; connected homes; remote telematics for almost anything with an engine; fleet management; cargo tracking; personal wearable devices for health and fitness and for medical uses; and drones, just to name a few. The applications and

---

[1] AT&T Services, Inc. submits these comments on behalf of itself and the other affiliates of AT&T, Inc. (collectively, "AT&T").

technologies are complex and diverse, and the potential for new IoT applications seems almost limitless. Like the app economy that sprouted in response to smart phones over the past decade, the Internet of Things presents immense opportunity for entrepreneurs and small businesses. With nearly ubiquitous wireless connectivity, Application Programming Interfaces (APIs) and off-the-shelf radio modules and other electronic components, inventors have already been developing a host of innovative new devices and applications that will bring new levels of efficiency and productivity to many different segments of our lives and the economy.

As NTIA itself recognized in its request for comments, the number of connected devices, already large, will grow exponentially, with a correspondingly dramatic economic impact. But this future is not inevitable. The same study cited in the Request for Comments that highlighted the economic opportunities inherent in the IoT also noted that the failure to adopt the right industrial and governmental policies to foster growth could reduce the prospective impact of IoT by nearly two-thirds.[2] One fundamental, enabling technology for the IoT is ubiquitous wireless connectivity, and support for IoT products and services will continue to demand massive investment in ubiquitous, highly secure, high-speed, low-latency, smart, software-defined networks. However, the investment needed to expand, maintain, upgrade, and protect these networks is extraordinary – AT&T alone announced plans earlier this year to invest nearly $10 billion in 2016 to deliver our integrated solutions to businesses around the globe.[3] An uncertain,

---

[2] *See James Manyika et al, Unlocking the Potential of the Internet of Things, McKinsey & Co. (June 2015), http://www.mckinsey.com/insights/business_technology/the_internet_of_things_the_value_of_digitizing_the_physical_world ("McKinsey Study),* at 2 and 101 (calculating a "low end" economic impact of $3.9 trillion for IoT, and describing the barriers to achieving the "high end" of $11.1 trillion).

[3] Jeanne Wassem, "Nearly $10 billion investment paves the way to our global leadership," Feb. 23, 2016, *available at*

incoherent or regressive regulatory climate could undermine incentives for continuing this critical investment, irretrievably dampening the prospects for IoT innovation. A primary goal of the Department of Commerce thus should be to foster the market conditions that will encourage continued deployment and upgrading of the massive, investment-intensive, smart networks that will be necessary to power the IoT.

Further complicating the task facing policymakers is the fact that the issues presented by the IoT are as diverse and complex as the ecosystem itself, presenting challenges unique to a particular industry vertical, like automotive safety, as well as those, like privacy and security, that cut across all sectors of the IoT. Thus, the critical question for policymakers is how to address these issues in a way that facilitates the efficient growth of IoT so that consumers, businesses, and government institutions in the United States and across the globe can achieve the economic and social benefits that IoT can bring.

AT&T thus welcomes NTIA's inquiry into the proper role of the government in fostering the advancement of IoT. The Department of Commerce is uniquely positioned to establish a leadership role on IoT policy within the Federal government, and to use that position—informed by the results of this inquiry—to work with stakeholders across the ecosystem, both within the United States and internationally, to establish a comprehensive, coherent, and consistent policy framework that will promote the continued development of IoT worldwide. To support that effort, AT&T draws on its multi-faceted experience as a leading global provider of IoT solutions—including wireless connectivity, devices, applications, platforms, security and more—to provide comments in response to the NTIA's inquiry. In these comments, we will (i) discuss

---

http://insider.web.att.com/s/editorial.dll?fromspage=hm/hm.htm&categoryid=&bfromind=1013&eeid=8191405&_sitecat=1654&dcatid=0&eetype=article&render=y&cincl=1.

AT&T's background and interest in the IoT, (ii) provide our view of some of the foundational concepts for the IoT, and (iii) explain how the DOC and other regulators can, with a carefully tailored and "light" regulatory touch, foster the growth of IoT devices and services while satisfactorily addressing legitimate public policy issues.

On that latter point in particular, we encourage the DOC/NTIA to use its leadership position on IoT issues to promote the development of a unified national policy framework for IoT that will minimize regulatory burdens and provide the certainty that will promote the on-going, robust network deployment and other infrastructure investment necessary to support this technology into the future. Accordingly, the DOC/NTIA should, at a minimum:

- **Establish a national policy framework to support continued investment in the next-generation network infrastructure that is necessary to support the IoT.**
  - Promote the deployment of broadband networks that will enable the ubiquitous availability of IoT services.
  - Eliminate regulatory barriers that impede the deployment of scalable next-generation IP networks that will enable secure and high-performance IoT services.
- **Support the collaborative, self-regulatory initiatives among industry stakeholders that have fueled the growth of the IoT to date.** Government should adopt a supportive, facilitating framework for IoT technologies.
  - Where there are industry best practices or voluntary frameworks already in place, agencies should respect and support them, rather than moving first to regulation. And where the development of new best practices and frameworks are necessary, the government should support industry-led or multi-stakeholder efforts in these areas.
  - In all cases the government should let competition, technology and customers drive this market, and avoid steps that would artificially channel developments along a particular path. In short, the government should adopt a "look-first before regulating" policy.

- **In those limited cases where regulatory action may be justified, provide for a light touch, flexible, well-coordinated regime that protects innovation and facilitates rapid IoT market developments.**
    - Any regulation must be applied with the lightest possible touch, and be competitively- and technologically-neutral. Moreover, given the dozens of agencies within the federal government whose responsibilities are implicated, either directly or indirectly, by the IoT, it is absolutely essential that any regulatory regime avoid duplicative and inconsistent regulation by multiple, overlapping agencies with different areas of jurisdiction.
    - The DOC can play a particularly important role as coordinator, keeping each agency focused on issues unique to its respective jurisdiction while working with industry to develop appropriate IoT-wide approaches for addressing policy issues that are common across the ecosystem, such as privacy and cybersecurity.
- **Advocate for an international, interoperable policy framework for IoT that facilitates the seamless global deployment of IoT products and services.** The Department of Commerce has a vital role to play in advocating for international policies that avoid unnecessary burdens on global IoT applications.
    - Foremost, all regulatory policy must protect cross-border data flows and avoid localized data retention requirements.
    - Regulators also must allow IoT providers to choose between various available options for numbering and device management, rather than imposing a single, one-size requirement for all cases.
    - As with domestic regulatory policy, the DOC should encourage international governments to promote the development of standards and operating frameworks for IoT that are developed through industry led, voluntary processes.
- **Support the progressive spectrum policies that promote the robust allocation of additional spectrum and the progress being made by industry and the standards bodies.** Although allocations of spectrum specifically for IoT uses are neither necessary nor helpful, continuing the overall process of making more spectrum available for both licensed commercial broadband and unlicensed uses is essential to ensuring the deployment and availability of the networks through which IoT solutions will be enabled.

DISCUSSION

I. AT&T IS AN INDUSTRY LEADER IN THE DEVELOPMENT AND DEPLOYMENT OF INTERNET OF THINGS SOLUTIONS

As early as 2008 AT&T established a business unit dedicated to connecting devices other than phones to its wireless network. That unit has developed into our current Internet of Things

Solutions organization focused on realizing the IoT for our customers. The company already has certified more than 2,600 connected devices—cellular IoT device types, as distinguished from smartphones and tablets—for use on our network. As of the end of the first quarter of 2016 nearly 27 million connected devices were connected to our network.[4] Reflecting the global nature of the IoT ecosystem, AT&T is providing IoT connectivity in more than 200 countries and territories.

AT&T is not resting on these accomplishments. Instead, we have been investing aggressively in our network in contemplation of the anticipated explosive growth in IoT. Over the past six years AT&T has invested $140B in its wireless and wireline networks, including the acquisition of wireless spectrum and operations. As of 2016, our 4G LTE network covers 350 million people in North America.[5] At the same time, we are transforming that network to handle rapidly changing customer needs and deliver new services, such as IoT. We are using newly purchased AWS spectrum that covers 96% of the US population to stay ahead of the strong growth in mobile data traffic. We are re-engineering the network to handle massive traffic volumes—in fact, we are planning for 10x growth in traffic volume across the network by 2020. And we are leading the industry in adopting a new Software-Defined Network architecture, which allows us to customize performance and security—including for IoT applications.[6]

---

[4] *See* https://www.business.att.com/enterprise/Portfolio/internet-of-things/?&WT.srch=1&source=EENT52MECGVPWn5vn&wtpdsrchprg=AT&T%20-%20M2M&wtpdsrchgp=ABS_SEARCH&wtPaidSearchTerm=+iot&wtpdsrchpcmt=+iot.

[5] http://about.att.com/news/wireless-network.html.

[6] *See* Andre Fuetsch, "Powering Ahead with our Software-Centric Network Transformation in 2016," Blog dated Feb. 23, 2016, *available at* http://about.att.com/innovationblog/022316mwc.

In short, IoT is a business priority for AT&T. The significance of the IoT to AT&T is pervasive. It factors into the company's plans for the continued deployment of core broadband network technologies and infrastructure, its need for and use of spectrum, and its participation in standards development processes. It embodies our mission to "Connect people with their world everywhere they live, work, and play—and do it better than anyone else." The results of these efforts are already showing in AT&T's support for specific IoT applications. The examples of our involvement span the IoT ecosystem.

- **Smart Cities**. In early 2016 AT&T announced the establishment of our smart cities framework, a holistic approach to helping cities better meet the needs of their citizens using IoT.[7] The framework, which will initially be deployed in select spotlight cities and universities, is supported by an alliance of key technology leaders and industry organizations. Together, we will develop and deploy solutions that help cities address critical issues like high energy costs, transportation, aging infrastructure, and public safety. Initial pilots include devices that monitor water quality in rivers; listen for and locate leaks in municipal water supplies; listen for, locate and identify the number and caliber of gunshots; and control street and traffic lights.
- **Connected Cars**. AT&T has been at the forefront in the development and application of IoT technologies in automobiles, which hold great promise for increasing safety and efficiency. AT&T connects more than 7 million cars in the US and Europe and has relationships with 19 car brands. We expect that more than 10 million cars will be connected to our network by the end of 2017.[8]

[7] "AT&T Launches Smart Cities Framework with New Strategic Alliances, Spotlight Cities, and Integrated Vertical Solutions," Press Release dated Jan. 5, 2016, *available at* http://about.att.com/story/launches_smart_cities_framework.html.

[8] *See* http://about.att.com/sites/internet-of-things/connected_car.

- **Cargo Tracking**. Underscoring the international nature of the IoT ecosystem, AT&T is working with Maersk to track and monitor the condition of over 280,000 refrigerated shipping containers with perishable goods around the world.[9] We also offer a device and platform (AT&T CargoView with FlightSafe®) that helps customers monitor shipments across road, rail, sea, and air.[10] Our customers range from agricultural producers like Monsanto to fine art transporters like Racine Berkow Associates.

- **Unmanned Aircraft Systems**. At February's Mobile World Congress in Barcelona AT&T announced an agreement with Intel to investigate adding 4G LTE connectivity to unmanned aerial systems (better known as drones), which would be a key element in enabling them to fly farther and more safely than ever before, consistent with FAA regulations.[11] Beyond increasing the range of UAS operations, adding LTE connectivity could also permit the development of new capabilities on the aircraft, such as video streaming, or transmitting diagnostic, telematics and flight information.

- **Connected Homes**. Our IP-enabled Digital Life service enables customers to increase the energy efficiency, security and convenience of their homes. That service is already available in 84 U.S. markets, and the Digital Life platform connects a plethora of security and automation devices to customers' homes. The service is expected to go international, as UK carrier O2 has announced plans to offer AT&T's Digital Life Services under its own brand in Europe.

- **Fleet Management**. Nearly 5 million active fleet management systems were in service in North America in 2014, and AT&T connects 1.9 million of these systems today. Working with AT&T, one customer—B&P Enterprises—saved $86,000 annually on insurance costs and reduced Department of Transportation violations by 80%.[12]

---

[9] "Maersk Teams with AT&T to Track and Monitor Cold Shipping Containers," Press Release dated Sept. 29, 2015, *available at* http://about.att.com/story/maersk_teams_with_att_to_track_cold_shipping_containers.html.

[10] *See* https://www.business.att.com/enterprise/Service/internet-of-things/asset-management/iot-cargo-view.

[11] "AT&T and Intel® to Test Drones on LTE Network," Press Release dated Feb. 22, 2016, *available at* http://about.att.com/story/att_and_intel_to_test_drones_on_lte_network.html. The FAA currently limits UAS operations to visual line of sight.

[12] *See* "AT&T Fleet Management Case Study – BP Enterprises," *available at* https://www.youtube.com/watch?v=sBsCg2OZmWc.

- **Health and Fitness Wearables**. The data generated from wearable devices allow consumers to monitor a broad range of biometric data, improve their health and wellness routines and share data with their trusted circle as well as their doctors. In February 2016 AT&T announced a new Foundry at the Texas Medical Center dedicated to digital health innovations that benefit those in and out of the clinical care environment, helping caregivers and patients bridge the gap between a clinical setting and the home.[13] To further help address the increasing demand on limited clinical resources AT&T also offers Remote Patient Monitoring, a mobile solution that virtually connects at-risk patients with their health care providers through interactive mobile devices.[14]
- **Telematics**. AT&T connects the Red Bull Formula One race cars—each equipped with up to one hundred sensors—and trackside engineers with the operations room at the factory in the UK, no matter where the cars themselves are racing. Over the course of a race weekend, AT&T will transmit up to 400GB of data.[15] These same capabilities can be brought to bear on many types of complex machines, from manufacturing to agriculture.

We do not detail these accomplishments to brag, although the company certainly is proud of its leading role nationally and internationally in making the IoT work for our customers. Rather, this work has given us insight into the technology and economics of the global IoT marketplace that inform our responses to the NTIA's inquiry and that, as we share below, should also inform the agency's approach to fostering the continued growth of the IoT and the enabling, smart network infrastructure that is necessary to support it.

II. A COMMON CONCEPTUAL AND DEFINITIONAL FRAMEWORK FOR THE IOT IS IMPORTANT TO NTIA'S INQUIRY

We believe it will be informative for NTIA's broad consideration of the IoT to provide an overarching view of how AT&T approaches the technology and business models of the Internet of Things, as well as the associated policy issues.

---

[13] "AT&T Foundry For Connected Health To Open At Texas Medical Center Innovation Institute," *available at* http://about.att.com/story/foundry_for_connected_health_texas_medical_center.html.

[14] "Remote patient monitoring: Helping bridge healthcare's gaps," *available at* http://www.corp.att.com/healthcare/docs/remote_patient_monitoring.pdf.

[15] "AT&T and Red Bull Racing," *available at* http://www.corp.att.com/latin_america/insights/irbr.

A. IOT TECHNOLOGY

From a technological perspective, IoT can be thought of as operating in the three "horizontal" domains described below. At least one element from each horizontal domain is necessary to assemble any IoT solution or service. The specific technologies within each domain are combined to deliver a "vertical" use case. These combinations also are not necessarily exclusive: the same network may connect many devices to multiple platforms, and platforms may use multiple networks to combine inputs from a diverse array of devices. While these domains exist in all IoT applications, it is important for policymakers to adopt frameworks that take an end-to-end approach to these technologies and apply consistently across the distinct domains.

- The **Device Domain** includes the physical devices—the "things" (like sensors and actuators)—that send data and respond to requests, creating an action or reporting data on something taking place in the physical world.
- The **Network Domain** includes the range of networks that connect devices in the device domain to a platform or application. This is **not** limited to commercial cellular networks. To the contrary, some industry estimates suggest that perhaps 5 billion of the 50 billion "things" to be connected to the IoT by 2020 will be directly connected to a cellular network. IoT devices will also connect over many other available types of networks. In addition to cellular LTE and 5G, the IoT will encompass devices on Wi-Fi, satellite, mesh or low power networks on unlicensed spectrum, and wired networks—and in some cases multiple different connection capabilities will be incorporated in a single device.
- The **Platforms and Applications Domain** includes the range of systems that receive data from or transmit instructions to IoT devices, analyze IoT device-originated data, provide an interface for the IoT device(s) and the data derived from them to human users, or link certain devices together.

Use cases are generally thought of as "vertical" solutions that provide a specific capability. Each vertical use case combines selected technologies from each horizontal domain to deliver a specific Internet of Things solution or service. There are multiple different technical pathways to providing that capability, depending on which technologies from each of the horizontal domains are employed in a given vertical use case. For example, with a connected

car, the Device Domain may include telematics sensors and a Wi-Fi hotspot in the car; the Network Domain may include a commercial cellular network; and the Platforms and Applications Domain may include the provisioning systems, interfaces, databases and other platform elements that the car manufacturer uses to interact with the car and, separately, that the car owner uses to interact with the telematics and Wi-Fi hotspot features and services associated with the car.

B. IOT BUSINESS AND ECONOMIC MODELS

1. IoT Business Models

Industry uses a wide array of different and still-evolving business models in the IoT ecosystem today. Below, we describe some of the more common business models, but we note that these models are constantly changing as the IoT marketplace continues to develop at a rapid pace.

- **End-to-End (E2E) services:** One provider manages the overall IoT service and experience through all three IoT domains. Typically, the IoT provider sells this as a branded solution, sourcing the devices, network access, and platforms from a variety of vendors or suppliers, but exerting sufficient management to present the IoT solution as an integrated and complete service to the customers—whether in business or consumer markets.

  > AT&T's Digital Life home security and automation service is one example of an E2E IoT solution. AT&T selects, sources, and offers the devices used throughout the customer's home (such as door/window sensors, door locks, cameras, temperature/water sensors, thermostats, and more), professionally installs them, provides a connection between the Digital Life controller in the home (which in turn connects to the devices throughout the home) and AT&T's 24/7 monitoring centers, and provides the apps and backend platforms that enable customer access to and control of their home's devices.[16]

[16] Although Digital Life is available as an E2E service, AT&T has also collaborated with third-party device manufacturers to give customers the option to connect separately purchased devices (e.g., thermostats and lighting) to the Digital Life platform via APIs.

- **Partnered Services:** Multiple parties cooperate or coordinate to deliver a set of IoT services and/or capabilities to the end users. These may be co-branded by the partnering firms, or even be provided as parallel independent offerings using shared capabilities in the device and network domains.

> Connected car services, enabled by AT&T's 4G LTE connections in the vehicles, are an example of partnered services. A car manufacturer offers owners of its cars a suite of telematics services that are connected by AT&T's wireless network to the manufacturer's IoT platform. The manufacturer may also offer car owners a Wi-Fi hotspot in the car that likewise relies on the car's AT&T-supplied 4G LTE connectivity. Customers can choose to purchase telematics services from the manufacturer, as well as Wi-Fi hotspot service from AT&T either on a stand-alone basis or as an add-on to an existing Mobile Share Value plan from AT&T. In this way, the two companies have partnered to offer parallel and complementary IoT services to customers using the same device and network domain elements.

- **Ad-hoc Solutions**. Here, the customer selects and assembles the elements of the IoT solution to create or to leverage an ad-hoc use case. The customer will often select a device—which may or may not have a companion application or service platform—and use its own existing network connectivity (mobile or fixed broadband) to enable the solution.

> Ad-hoc solutions naturally take on many forms. For example, in many health and fitness use cases, a consumer may purchase a wearable device to monitor steps, heart rate, and other data that is relayed via Bluetooth to an app on a smartphone, which in turns uploads the data via a cellular data connection over the Internet to an IoT service platform that may or may not be provided by the entity that manufactured the wearable device. The consumer may purchase a separate device, like a Wi-Fi scale, that independently takes weight and body fat percentage readings, and uploads them over Wi-Fi and the consumers' home wired broadband connection to the same—or possibly even a different—IoT service platform. In this way, the consumer is piecing together a more complete view of their personal health and fitness that may be consolidated with a single IoT service provider—or spread across multiple 'best-of-breed' options for the specific health tracking/analysis functions (e.g. Strava's platform for aggregating data from different brands of fitness trackers).

2. Economic Effects

a. Successful Deployment of IoT Solutions Requires Changing Business Models for Many Industry Segments—And Thus More Flexible Regulatory Approaches.

Consideration of the economics that shape the IOT is also critical to the DOC's work in this area, particularly to promoting the further development of the IoT marketplace in the United

States and globally. As noted above, there are a variety of business models competing to deliver any given IoT solution or capability to the market. Each business model implies a different set of firms with differing means of deriving revenue from a particular IoT service. Equipment or devices sales; network connectivity services; application sales; platform subscription services; advertising; and data analysis are just some of the ways in which firms seek to earn money from IoT services. The diversity of use cases and the evolving value associated with differing components of IoT solutions changes the economics of certain industry segments within the different IoT technology domains.

i. Device Domain: Equipment Manufacturing and Device Sales

Equipment and device manufacturers—from watch to thermostat to automobile manufacturers—see adding connectivity and intelligence to those items as a means of significantly increasing their value, justifying higher prices and potentially (subject to the intense competition being experienced in many device categories) higher margins for previously low margin products. For example, while a traditional non-programmable "dumb" thermostat can easily be purchased for $20-$40, a Wi-Fi enabled "smart" thermostat, enabling remote access and a host of new energy-saving and convenience factors, may sell for several hundred dollars. Similarly, as many manufacturers move from a straightforward unit sales model to one in which they provide and support a platform as part of an IoT offering, they are adding connectivity subscriptions and other services to their business models as new sources of revenue.

ii. Network Domain: Broadband and Mobile Network Operators (MNOs)

The market for MNO IoT solutions differs significantly from the market for traditional mobile end-user service for several reasons. First, most IoT network traffic presents a very different profile from standard voice and data services. It is frequently very low-bandwidth and

delay-tolerant traffic (e.g. routine reporting from a remote sensor in an industrial setting). Consequently, pricing is typically quite low, with low average revenue per connected device.

Second, in many IoT solutions MNOs do not provide a communications service directly to individual end users. Rather, they provide wireless connectivity to the providers of IoT devices and/or platforms, who incorporate connectivity into their product or service offering. The IoT device provider, in turn, does not typically hold itself out as providing traditional communications services, but rather offers a device performing a specific function that is enhanced by the integration of wireless connectivity. A smart meter measures electricity usage; the built-in connectivity allows the continual transmission of usage information to the utility. Moreover, the device provider typically does not charge the end user for a stand-alone communications service; data transport is merely an ancillary component of the overall product or service (e.g. data analytics, fleet management) sold to the end-user customer.[17]

Third, the geographic demand for network coverage for IoT solutions also commonly differs from traditional demand for coverage for traditional phone usage. Coverage for traditional consumer devices is determined by population—where the people are. In contrast, IoT solutions can drive coverage requirements to just about anywhere, particularly in the case of remote monitoring applications. This, over time, will influence both the network technologies chosen (such as the possible incorporation of satellite connectivity) and the capital allocation for continued wireless network build out—but in the face of the reduced average revenue per connection noted above.

---

[17] To be sure, there are exceptions to this general rule, but in AT&T's experience they are relatively infrequent.

Finally, there is the increasing demand for global deployment. With device manufacturers looking to sell globally, the complexity of global deployment across numerous mobile operators is daunting, especially for those solutions with embedded cellular connections (like connected cars, asset management, and industrial or agricultural equipment). This is discussed further below.

iii. Platform Domain: Applications and Services Providers

The platform domain of the IoT tends to offer the greatest diversity of revenue models. Many consumer oriented applications and platforms exhibit the range of business models typical to any set of mobile or web apps: free (with purchase of a device), free with advertising, "freemium" (with advertising that is eliminated by an upgrade), or subscription-based. Enterprise and industrial platforms may be offered in the context of broader service arrangements and complex deals, incorporating data analytics, device management and provisioning, application or data hosting, and additional (non-IoT) business or enterprise services. Two-sided market opportunities are also prevalent in IoT solutions offerings. For example, end-users may get free access to an IoT service platform in exchange for consenting to sharing data from their service to and/or through the service provider, and the IoT service provider in turn derives revenue off of that data in any of a variety of possible ways, such as advertising or the sale of analytics to third parties.

b. Economics of Complete IoT Solutions

In the IoT ecosystem, economies of scale are essential for a number of reasons:

- **Devices**. To efficiently amortize their costs, IoT device manufacturers tend to develop standardized products with long useful lives that can be sold in very large volumes across many countries. Because their devices or products usually have very low average revenue per user (ARPU), particularly in comparison to cellphones and tablets, IoT device or product manufacturers are extremely sensitive to development and deployment input costs. These are typically reduced through increased scale.

- **Network Providers**. Again, in comparison to cellphones and tablets most IoT devices typically have low data consumption and very low ARPUs. For example, a smart meter usually will transmit a few hundred bytes of data per day, while a smartphone or tablet may consume scores of megabytes or even gigabytes per day.
- **IoT Solutions Providers**. As noted earlier, IoT solutions providers—whether the device maker or strictly a platform provider—typically do not sell, or charge end users separately for, wireless connectivity. Instead, wireless connectivity is often included in the overall price of the IoT solution. Many IoT solutions benefit from "network effects" when a particular IoT platform is adopted by a larger number of users—i.e. the value of the IoT platform to both its provider and its users goes up with the number of people using a given platform. For example, scale enables better data analytics through larger data sets (which in turn enables better insights to be provided to end users or other parties). Larger platforms can also attract users based on a greater ability to integrate a broader array of devices or other elements of the IoT solution.

To be successful in the face of these economic realities, IoT device manufacturers must be able to "***build it once—sell it everywhere.***" IoT network connectivity providers in turn must be able to provide connectivity virtually anywhere and everywhere to attract IoT customers. And IoT platform providers must grow their base of users to continually improve their offerings.

i. Problems With Applying Traditional Business Models to the IoT

Given the unique and challenging economics of the IoT marketplace, IoT device manufacturers would face an almost insurmountable obstacle when seeking to deploy IoT products and services on a global scale if they were required to follow the traditional business models for mobile handsets and tablets. For example, to obtain wireless connectivity under those models, an IoT device manufacturer would need to contract with a separate MNO in each country into which it sells its goods, which likely would mean incurring transaction costs for negotiating dozens or even hundreds of individual agreements. Moreover, for each country, the IoT device manufacturer would need a Subscriber Identity Module ("SIM") card embedded with

a country-specific International Mobile Subscriber Identity ("IMSI") code for each IoT device to be distributed in that particular country, leading to increased inventory management costs.

Requiring an IoT provider to use country-specific numbering resources would pose yet another impediment to the successful deployment of a product. Such a requirement would force the IoT device manufacturer to forecast customer demand in each country with extreme precision to avoid having too few or too many IoT devices with a SIM card properly coded for a particular country. Multiplied across dozens or hundreds of countries, the administrative costs and operational complexities of manufacturing the "right" number of IoT devices with the "right" SIM and distributing them to the "right" country could quickly become overwhelming.

In addition, each MNO would likely have its own ordering, provisioning and billing platform. The IoT manufacturer would need to have the capability to interface with and navigate each of these disparate platforms. This would impose additional costs on the IoT manufacturer as it established each operator-specific interface and gained the necessary expertise to work with multiple MNO systems. It also would reduce operating efficiencies for the IoT manufacturer because the data from the various MNOs would be collected differently and could not readily be consolidated and analyzed under identical parameters across multiple countries. These issues would only be exacerbated by the pernicious effects of data localization requirements or restrictions on cross-border data flows. At a minimum, these obstacles would substantially raise input costs and slow time to market. At worst, these added costs would break the business model to ever deploy certain devices in multiple countries.

ii. IoT Stakeholders Are Using New Business Models and Negotiated Arrangements to Successfully Provide Wireless Connectivity for IoT Solutions Globally.

The IoT device manufacturers and the wireless industry have responded to these various challenges with innovative business models and commercially negotiated IoT roaming agreements that have facilitated the deployment of IoT technologies across the globe.

The Global SIM. In order to achieve the necessary economies of scale, IoT device manufacturers often seek to partner with a single MNO that can deliver wireless connectivity in all, or nearly all, of the countries where the IoT manufacturer seeks to sell its products. By relying on a single MNO for its global wireless connectivity needs, the IoT device manufacturer can negotiate one wireless connectivity contract, use one Mobile Country Code ("MCC") and Mobile Network Code ("MNC") for the IMSIs in all of its SIMs, use E.164 numbers sourced from one MNO (if necessary for its IoT product), and use the ordering, provisioning and billing systems of one MNO in delivering its IoT products globally. This single platform, or "Global SIM," approach to IoT deployment substantially reduces barriers to market entry for IoT device manufacturers, particularly for those smaller entrants who would not otherwise have sufficient resources to compete on a global scale.[18] As discussed below, the wireless industry is already helping IoT manufacturers achieve their goals for efficient international operation with a variety of commercially available solutions.

[18] From the perspective of the IoT device provider, the desire to use a global SIM in this context is both logical and efficient. IMSI codes are merely a way to identify (i) the subscriber of the service (last 9 or 10 digits) and (ii) the network operator to whom the subscriber is subscribed (first 5 or 6 digits). E.164 numbers are merely an addressing scheme used to route calls to the appropriate destination. Using IMSIs and E.164 numbers sourced from a single MNO accomplishes the twin numbering goals (identification and addressing) in a much simpler, cost-effective manner than would be possible using traditional business models with IMSIs and E.164 numbers for each country.

International Wireless Connectivity Built on the Same Foundation as Traditional Voice Roaming. The wireless industry has responded to the need for efficient IoT numbering solutions with commercially negotiated roaming agreements that specifically address the provision of IoT services. Historically, MNOs have supported their customers' international wireless connectivity through roaming agreements with MNOs in other countries.[19] To facilitate the adoption of these types of international roaming arrangements, the wireless industry's leading trade association, the GSM Association (GSMA), has developed a series of roaming contract templates. They are available to GSMA's 800+ members and contain common industry accepted terms and conditions that expedite the negotiation of roaming agreements. Negotiations often involve only price, and not the other industry accepted terms. As a result, commercially negotiated roaming arrangements that enable these customers to receive service outside their home country have been in place for decades and are mutually beneficial to the MNOs: the MNOs' customers receive service in foreign countries and the MNOs receive compensation from the other party for providing the service.

M2M Roaming—The Industry's Transparent Framework. Building on its success in fostering traditional roaming, GSMA in 2012 adopted an "M2M Annex" template for international M2M roaming. Among other things, this contract template mandates transparency in the provision of M2M/IoT services by requiring the parties to the agreement to identify their M2M/IoT traffic separately from other traffic. Taken together, international roaming agreements

[19] For example, MNO A in Country A agrees to provide wireless services to the customers of MNO B from Country B when those customers are located within MNO A's network footprint. Importantly, MNO B's customers remain MNO B's customers even though they are being served by MNO A's network. Moreover, while roaming on MNO A's network, MNO B's customers will necessarily be using devices with IMSIs and E.164 numbers that are associated with Country B because they purchase the wireless service from their home operator in Country B. In other words, they will be using IMSIs and E.164 numbers extraterritorially.

and the M2M Annex provide an industry-wide standard contractual structure for supporting IoT services globally. [20]

Today, AT&T has bilateral roaming agreements in place with MNOs worldwide. These agreements support the provision of international IoT services, with virtually all agreements using the GSMA M2M Annex. Pursuant to these agreements, the MNOs, their IoT customers, and the customers' end users enjoy the benefits of international M2M roaming in each other's country. These types of arrangements are fast becoming the norm in the industry, and their continued development and use on a voluntary, mutually-negotiated basis should be encouraged.

C. IOT AND GOVERNMENTS

1. Roles of Governments

Governments at all levels within the United States—federal, state, and local -- as well as governments internationally, are notable stakeholders in the IoT, and each can play multiple roles in that system. These roles generally can be grouped into five categories:

- **Customer**. Federal, state, and local governments all have shown an increasing interest in a broad variety of IoT solutions, from public safety and law enforcement (e.g., remote cameras, gunfire detectors), to telematics for fleet management, to sensors and monitoring equipment for real estate and other physical facilities. In short, just about every government organization will have use for IoT capabilities in their everyday work.

[20] Notwithstanding the acceptance of roaming for the delivery of IoT services, roaming should not be viewed as the only means to facilitate the provision of international IoT products and services. So long as the parties mutually agree, MNOs should have the flexibility to develop other commercial arrangements whereby IoT services are supported via the extraterritorial use of numbering resources (e.g., resale).

- **Funder &/or Facilitator**. Governments at all levels may allocate or appropriate funds for programs that in turn may be disbursed to government customers. For example, federal funding may be made available to state governments through grant programs that enable states to purchase or deploy IoT services or solutions. Alternatively, governments may control access to infrastructure (e.g., rights-of-way, streetlights) that may be needed to support IoT deployments. In these and other ways, governments can greatly affect the availability and use of IoT solutions.
- **Influencer**. Through research, inter- and intra-governmental coordination, and other activities that are neither regulatory nor directly involve acquisition, governments inevitably influence the development of the IoT ecosystem.
- **Regulator**. Agencies with explicit or implicit regulatory authority over certain aspects of IoT-related products and services may seek to exercise that authority to prescriptively regulate aspects of those services
- **Enforcer.** Agencies with enforcement powers that either explicitly encompass the IoT or at least address policy issues implicated by it may seek to apply existing authority toward alleged violations of current statutes or regulation by providers of IoT capabilities. In some instances, such an exercise of enforcement is a natural and appropriate application of generalized enforcement authorities traditionally rooted in consumer protection issues, such as those exercised by the Federal Trade Commission (FTC) and the Department of Justice. In other instances, agencies that regulate a single sector, such as automobile safety, have begun to take expansive views of their powers in ways that may affect the rest of the IoT as well. Some states' Attorneys General have also sought to bring enforcement actions with regard to IoT products and services.

2. IoT and Policy Issue Categorization

Finally, although public policy issues will be addressed more fully below, it is useful here to categorize policy issues in terms of their relationship to IoT services and verticals. This is important to help stakeholders recognize when an issue they are considering may or may not have an impact elsewhere within the IoT. From AT&T's perspective, these fall into three categories:

- **Issues common across all IoT solutions, such as security and privacy.**
- **Issues common to all IoT verticals but that have some unique manifestations in specific verticals**. For example, automotive cybersecurity has implications for the issue of automotive safety, with concerns that present some unique considerations that differ from the security of computers, smartphones, or consumer electronics.

- **Issues unique to specific verticals** (for example, flight safety rules for UAS), for which the policies adopted do not significantly impact other verticals.

Properly categorizing a given use case can at times be a challenge for government and industry alike, but doing so is crucial to determining who the appropriate governmental, industry, and end-user stakeholders in the policy considerations are or should be. It is also crucial to fully assessing the proper scope and impact of the policies under consideration.

III. THE DOC SHOULD TAKE THE LEAD IN DEVELOPING A NATIONAL POLICY FRAMEWORK FOR THE IOT THAT PROMOTES NECESSARY INTRA- AND INTER- GOVERNMENTAL POLICY COORDINATION AND INFRASTRUCTURE DEPLOYMENT

It is important to recognize that, much as was the case with the Internet's commercial development, the developments in IoT technologies and the global spread of IoT business largely have been achieved in the absence of, not because of, government oversight and intervention. The innovation that has fueled the explosive growth in IoT technologies to date has been the result of private sector investment, in a climate of slight, if any, regulatory oversight. Accordingly, it is vital for the Department of Commerce to set a national policy framework that will support the continued, aggressive investment in the next-generation network infrastructure necessary to power the IoT. Over-regulation of communications networks will slow the deployment of the ubiquitous, next-generation networks over which the IoT will ride as it develops over the coming years. For years now, AT&T has been making more domestic investment than any other American company, all with an eye to deploying the smart, secure, robust, software-defined network that will serve as a foundation for broad-based, national economic growth. We encourage the Department to adopt policies with respect to the IoT that will help to support the continuation of this network investment more generally.

Beyond these important issues of infrastructure deployment the policy landscape is growing more complex in other ways. As IoT solutions gain adoption across a greater range of

market and industry segments, and at greater scale, many stakeholders in the IoT ecosystem are finding themselves engaged with a broad array of federal agencies with varied roles, levels of experience, expertise, and confusing and sometimes conflicting regulatory and enforcement authority regarding IoT. This situation is mirrored both at the state and local levels of government domestically, and abroad with myriad foreign governments and international institutions.

Depending on how one counts, hundreds of federal entities could play some role in the IoT ecosystem. Some, such as the FTC, the Department of Commerce's own NIST and NTIA, as well as various agencies within the Departments of Transportation and Homeland Security, have already taken conscious and explicit steps to get involved in the IoT across each of the five capacities outlined above. In some cases agencies have essentially backed into their involvement, as new regulations or other actions promulgated for other purposes have had unanticipated collateral effects on the IoT.[21] And still other agencies -- NHTSA with connected cars and the FAA with UAS are examples -- have worked to keep up with IoT technology, as developments in the IoT space have sped ahead of efforts to address issues through the regulatory process. This creates uncertainty about the agencies' approaches to the issues and about the IoT business opportunities in these sectors. For its part, Congress has also repeatedly

[21] For example, the Food and Drug Administration recently published a final rule on Sanitary Transportation of Human and Animal Food, under the Food Safety Modernization Act (FSMA), which requires that vehicles used to ship food must be capable of maintaining temperatures necessary for the safe transport of food. The rule requires that vehicles and transportation equipment used for food "requiring temperature control for safety must be designed, maintained, and equipped as necessary to provide adequate temperature control to prevent the food from becoming unsafe." This has created opportunities for IoT solutions to facilitate compliance with the new regulation. Although the final rule eliminated the proposed rule's *requirement* for temperature recording device to be installed in cold storage compartment (*see* https://www.federalregister.gov/articles/2016/04/06/2016-07330/sanitary-transportation-of-human-and-animal-food#p-389), compliance with the final rule can still be better facilitated by an IoT temperature monitoring and reporting device—which is a typical function of an IoT asset management solution.

expressed interest in the IoT through hearings, resolutions, legislation, and even the establishment of both the Congressional Internet of Things Caucus and a Bipartisan Internet of Things Working Group, [22] all within the last two years.

Given the unprecedented breadth of IoT services, and their impact across virtually every sector of the economy, the assortment of agencies implicated by the IoT is not surprising. Nevertheless, the great potential for regulatory confusion through duplicative and inconsistent rules and enforcement—and, in turn, for detrimentally affecting innovation and investment in IoT technologies—is a significant cause for concern for industry stakeholders. As a counterpoint, the significant benefits that governments at all levels and across many entities stand to gain through adoption and use of IoT solutions in government functions is a significant opportunity for government, industry, and society more broadly.

The potential for negatively affecting private sector investment in the networks and communications technologies that are essential to the IoT marketplace must be at the forefront of our national policies: after all, it is the *Internet* that puts the "I" in IoT. For example, one of the foundational elements of the IoT is mobile wireless connectivity. Ubiquitous wireless networks have been an essential enabler to the explosive growth in the IoT ecosystem—much of which is tightly intertwined with the mobile app ecosystem that has grown so tremendously over the last decade. But as noted earlier, the investment needed to expand, maintain, upgrade, and protect these networks is massive, and far from an inevitability—especially if regulatory headwinds force providers to explore alternative uses for scarce capital.

---

[22] "Latta and Welch Launch Bipartisan Internet of Things Working Group" *available at* https://energycommerce.house.gov/news-center/press-releases/latta-and-welch-launch-bipartisan-internet-things-working-group, May 24, 2016.

The DOC and NTIA thus should seek to foster a coordinated national framework for the IoT that minimizes regulatory burdens, provides policy clarity and certainty, creates a climate that maximizes this enabling network infrastructure investment, and recognizes the global nature of the IoT. In furtherance of that policy framework, DOC/NTIA could launch an interagency process whose goal will be to help the federal government align and harmonize agency initiatives that affect the IoT.[23] Adoption of such a policy framework – and cross-agency process -- will facilitate the continued investment in and deployment of the highly secure, dynamic, software-defined-networks that providers like AT&T have been working for years to build—and that will be increasingly necessary to support the dense network requirements of the IoT in the future. We discuss below several key attributes of such a national policy framework that can help ensure the on-going, robust network deployment and technology development necessary to support the continued growth of the IoT into the future.

A. THE POLICY FRAMEWORK SHOULD SUPPORT AND ENCOURAGE THE DEVELOPMENT OF SOLUTIONS THROUGH VOLUNTARY, COLLABORATIVE INITIATIVES AMONG MULTIPLE STAKEHOLDERS.

As the example of M2M roaming described earlier shows, industry players have risen to the challenges presented by the necessity for seamless international deployment of IoT

[23] There are several models for such an effort at cross-agency coordination. For example, the new Federal Privacy Council, which is managed out of the Office of Management and Budget, has been established as a way to promote a comprehensive and consistent program on privacy among various federal agencies. *See* https://www.whitehouse.gov/blog/2015/12/01/prepared-remarks-omb-director-shaun-donovan-federal-privacy-summit. Similarly, The GPS National Executive Committee, which is run out of the National Coordinating Office (and hosted by DOC), features a permanent staff that is charged with coordinating GPS policies. *See* http://www.gps.gov/governance/excom. Given the current and expanding importance of the IoT to the national economy, adopting a similar structure and process for reviewing and coordinating regulatory actions that bear on the IoT certainly is worthy of serious consideration.

technology through a process of voluntary negotiation and innovation.[24] The Government's policy framework should prioritize support for such efforts. Thus, where there are industry best practices or voluntary frameworks already in place, the government should respect and support them. Where new standards or policies are necessary to address evolving issues, rather than moving immediately to prescriptively regulate, government can encourage—and, in some cases convene—multi-stakeholder initiatives as the first step in addressing issues associated with newly emerging IoT applications or technologies. But the policymakers must resist the temptation to reactively prescribe a "solution" for these issues that risks artificially skewing the development of the market or technology development. Instead, regulators should let competition, innovation, and customer demand drive developments in the IoT marketplace.

In no case should policymakers encumber the IoT with legacy regulations that were never designed for it, such as Federal Communications Commission (FCC) regulations designed for legacy telephone markets. If policymakers limit the opportunity for network operators to explore new market opportunities, they make investment more difficult and risky. Regulatory policies that allow permissionless innovation encourage all players to pursue every conceivable market opportunity. Promote investment and innovation, and consumers will benefit.

[24] There are numerous examples of successful industry-led or multi-stakeholder efforts to confront policy issues affecting the IoT. In the case of cybersecurity, the NIST Framework was developed with input from government and private industry stakeholders, resulting in a vehicle that effectively addresses the cybersecurity posture of critical infrastructure and other entities. Other notable examples are the FTC privacy framework for IoT, NTIA's UAS privacy framework, CTA's wearables privacy principles and the Future of Privacy Forum's smart grid privacy principles. Several of these will be discussed further below.

B. IN THE LIMITED CASES WHERE REGULATION MAY BE NECESSARY, THE GOVERNMENT MUST APPLY A "LIGHT-TOUCH," FLEXIBLE, AND WELL-COORDINATED REGIME THAT PROTECTS INNOVATION AND FACILITATES RAPID MARKET DEVELOPMENTS.

In the rare cases in which regulatory intervention may be appropriate, government should ensure that it is as light-touch as possible. Just as importantly, especially in view of the myriad agencies and other government entities with a potential interest in the IoT market, policymakers must guard against both duplication and inconsistent application by multiple, overlapping agencies with different areas of jurisdiction.

Policymakers also must ensure that any regulation does not inappropriately tilt the IoT playing field. As the various business and technology models described above illustrate, there are many different ways in which comparable and competing IoT solutions can be delivered to end users. Legacy regulations and regulatory approaches are often constrained to certain technological or industry silos that do not accurately map to the current range of these IoT solutions. There have not yet been new statutes enacted that would reconcile the jurisdiction and function of many regulatory entities with the current reality of the IoT. Thus, particular care must be taken in developing any regulations that are intended to address concerns pertaining to the IoT or a vertical within the IoT; any such regulations must be competitively- and technologically-neutral, and should impose similar burdens and responsibilities across the IoT domains, end to end. They must also avoid singling out individual companies or business models for disparate treatment, whether favorable or unfavorable.

As the DOC/NTIA work to establish a coherent and consistently applied policy regime for the IoT, it is essential that they distinguish between unique, "vertical" issues that may fall within the purview of a particular expert agency, and "horizontal" issues that cut across the IoT ecosystem's verticals and that should be handled similarly across all IoT technologies, business

models, and use cases. It is here also that the proper identification and categorization of issues and their effects, as discussed above, must be considered: the most challenging situations are those in which there is a vertical-specific manifestation of a "horizontal" issue with some peculiar attributes that may legitimately call for some vertical-specific measures. However, these measures must be taken in consultation with a broad range of stakeholders, and in close coordination between the appropriate vertically oriented agency and a policy coordinating entity—like the DOC—to ensure that any resulting regulations are narrowly and appropriately applied, without undue effects on the broader IoT.

Examples of issues in the "vertical" bucket include airspace coordination for drones (subject to FAA jurisdiction), medical device certification (the FDA), and automotive safety (NHTSA). Each of these verticals, both in a business and regulatory sense, have varying propensities for overlap with other verticals, or for regulations applied to these verticals to have potential ramifications for the broader IoT.

Two prime examples of "horizontal" issues are security and privacy. These are natural concerns with every IoT use case, and indeed, consumers will rightly expect that their chosen IoT solutions will be secure and respectful of their privacy. Establishing this trusted environment for consumers will require work by all players in the IoT—device makers, connectivity providers, application developers, and platform operators; doing so will be crucial to their success in the market, separate and apart from the policy frameworks for these issues. With this broad variety of industry players, it will be impossible to regulate a path to effective privacy and security protection. Rather, those protections will depend on a robust multi-stakeholder process to define the practices that will engender consumer trust—and therefore adoption—across the system. Thus, for these horizontal issues, government should opt for a

common, IoT-wide framework that relies not on regulation, but rather on multi-stakeholder efforts—including the relevant expert agency—that will facilitate development of effective privacy and security approaches for the IoT.

1. Cybersecurity

The industry is already keenly focused on the security issues around IoT services. As devices become ever more connected, potential security vulnerabilities are likely to increase across the ecosystem. IoT security, therefore, is a necessity, but a prescriptive regulatory approach is not. Businesses will have significant incentive to address security from the outset in order to succeed in the marketplace.

In addition, there are a wide variety of standards bodies working on security specifications for the IoT. In the United States, the NIST Cybersecurity Framework should be the starting point on all security questions related to the IoT. The Framework is built around the concept of risk management, which we believe is the best means to address cybersecurity, particularly given the rapidly changing nature of the threats. The Framework can be a useful tool for companies to evaluate their cybersecurity risks and build a risk management plan specific to their business. The communications sector has undertaken a significant effort within the FCC's Communications Security, Reliability and Interoperability Council (CSRIC) to apply the Framework to communications critical infrastructure. That work encompassed ten subgroups and over one hundred individuals from a wide variety of companies, academic institutions, non-profits and government agencies, culminating in a report that was issued in March 2015. The industry also has undertaken a variety of activities to promote the Framework to other stakeholders in the communications sector, including both suppliers and smaller and mid-sized carriers.

AT&T itself employs a cybersecurity risk management program that predates the NIST Framework and that relies upon many of the same widely accepted, international security standards that map to the informative references in the Framework. We use these standards to inform our internal controls that we then apply to our network systems and to help protect customer data. Thus, the Framework serves as a complement to that program.

As AT&T recently noted in comments to NIST, the existing Framework is readily applicable to the IoT. Indeed, we recommended that NIST take steps to apply the Framework to a variety of issues that have come up since its publication related to IoT, including by developing use cases or examples of how the existing Framework can be used or applied in those environments. AT&T also has built on its experience with the Framework and the work we are doing with customers across many industries—as well as with our own IoT deployments—to promote better cybersecurity practices in the IoT ecosystem through a series of White Papers.[25]

2. Privacy

Any approach to IoT privacy should begin by examining the privacy implications of the IoT application in question, rather than treating all applications the same. Many IoT applications do not involve personally identifiable data and consequently present no meaningful privacy risk. Nevertheless, to the extent intervention is necessary, the FTC—the federal government's expert agency on privacy—alone should be tasked with ensuring appropriate privacy protections for the IoT and should proceed, as it typically does, through enforcement across the sector, rather than through *ex ante* rule-making. There is in fact no reason for prescriptive regulation here, as

[25] *See, e.g.*, "The CEO's Guide to Securing the Internet of Things," *available at* https://www.business.att.com/cybersecurity/

industry stakeholders already have been proactively engaged in voluntary and collaborative processes to provide appropriate privacy protections for IoT applications.

A case in point in the United States is the development of a Smart Grid Privacy framework. In October 2012, the Future of Privacy Forum (FPF) announced a privacy seal program based upon a fundamental set of privacy principles incorporated in its Smart Grid Privacy Guidelines.[26] Aware of the critical need for privacy and security protections for sensitive consumer energy information, industry members proactively engaged in collaborative, self-regulatory efforts. FPF convened a diverse group of companies—including AT&T—to develop the privacy framework. FPF also requested input from utilities and utility regulators as interested stakeholders.

The resulting Guidelines target companies that use consumer information to provide smart grid services (e.g., companies offering home energy management, remote home control or security, smart thermostats and other services). Furthermore, the Smart Grid Privacy Guidelines are designed to help assure consumers that organizations using their information are employing best practices for security, privacy, and dispute resolution and are using consistent approaches to obtaining consent. As the Smart Grid example suggests, self-regulatory measures can deliver real progress toward a more comprehensive, consumer-centric approach to privacy.[27]

---

[26] *See* https://fpf.org/issues/smart-grid/.

[27] An even more recent example of a successful multi-stakeholder approach to addressing privacy issues in the IoT is the process NTIA convened for UAS. That process resulted in a consensus document setting forth privacy best practices. *See* https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-unmanned-aircraft-systems.

The FCC's pending rulemaking to establish new privacy rules for broadband providers is illustrative of exactly the wrong approach to privacy:[28] applying one set of rules to one set of technologies and industry players (in this case, Internet Service Providers) that creates consumer confusion and different privacy requirements across the IoT ecosystem and the actors in each of its domains. This not only puts some industry stakeholders at relative disadvantages to others—based solely on technology and perceived regulatory jurisdiction—but also creates an artificially complex privacy regime for consumers, while potentially depriving them of beneficial IoT products and services that could be enabled with a properly tailored, more consumer-centric approach to privacy.

C. THE POLICY FRAMEWORK MUST SUPPORT AND FACILITATE THE SEAMLESS DEPLOYMENT OF IOT SOLUTIONS INTERNATIONALLY.

As detailed above, the economics of the IoT ecosystem make the frictionless deployment of IoT products and services across global borders a business imperative. The Department of Commerce thus has a vital role to play in advocating for international policies that reduce and avoid unnecessary burdens on global IoT applications. Government action on IoT must keep in mind the vital importance of cross-border data flows, and should not restrict the legitimate movement of data across national borders.

Even as it provides for the ubiquitous use of IoT technologies, government policy nevertheless must avoid prescribing specific marketplace solutions for effecting it. For example, in the case of numbering, ideal numbering policies and provisioning/activation models in particular can vary significantly across IoT applications. What works best in one application

---

[28] *See In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Notice of Proposed Rulemaking, WC Docket No. 16-106 (Rel. Apr. 1, 2016).

may not fit another. International regulators thus must permit IoT providers to choose between various available options for numbering and device management, rather than imposing a single, one-size alternative for all cases, and certainly not one that is determined or established on a country-by-country basis. [29] As the Global SIM and IoT business models described earlier in these comments clearly demonstrate, industry stakeholders are fully capable of addressing the business and technological challenges inherent in the international IoT marketplace through voluntary negotiation and innovation.

Finally, the DOC, along with international governments, should promote the development of standards and operating frameworks for the effective global deployment of M2M and IoT solutions. Indeed, the German government, working with private industry and other

---

[29] Regulators in several countries have taken an enlightened approach to the numbering issues presented by the IoT, such as by allowing the extra-territorial use of IMSI codes in the context of the provision of M2M Services and adjusting their numbering policies to make them more flexible to enable such extra-territorial use. For example, both the Belgian Institute for Postal Services and Telecommunications ("BIPT") and Germany's Bundesnetzagentur ("BNetzA") recently announced new policies that, when implemented, would permit the extra-territorial use of national numbers for IoT services. *See Summary and further analysis answers to the consultation at the request of the BIPT Council of 25 November 2014 on reviewing the policy regarding the numbering plan management of 28 July 2015* ("BIPT Summary"), *available at* http://www.bipt.be/en/operators/telecommunication/Numbering/regulation/summary-and-further-analysis-answers-to-the-consultation-at-the-request-of-the-bipt-council-of-25-november-2014-on-reviewing-the-policy-regarding-the-numbering-plan-management-of-28-july-2015; http://www.bundesnetzagentur.de/cln_1431/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Nummerierung/TechnischeNummern/IMSI/AnhoerungEntwurfIMSI.html?nn=268376 (BNetzA proposed regulations). Even more recently, at its meeting in El Salvador on May 17-20, 2016, CITEL, the Comisión Interamericana de Telecomunicaciones of the Organization of American States, approved a "Recommendation to Incentivize Greater Adoption of IoT/M2M Services in the CITEL Member States" which recommends "[t]hat the Member States allow for the extra-territorial use of numbering resources (i.e., E.164 and E.212 numbers) to support global IoT/M2M business models and the development of innovative products and services, while not compromising public security or national sovereignty." See CITEL document no. CCP.I-TIC/doc. 3905/16 rev.1, recommendation no. 4. *See also* Body of European Regulators for Electronic Communications (BEREC) Report on Enabling the Internet of Things, Dec. 2, 2015, *available at* http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5755-berec-report-on-enabling-the-internet-of-things; European Conference of Postal and Telecommunications Administrations ("CEPT"), Extra-Territorial Use of E.164 Numbers - High level principles of assignment and use, ECC Recommendation (16)02, Approved April 28, 2016, *available at* http://www.erodocdb.dk/Docs/doc98/official/pdf/REC1602.PDF.

stakeholders, has already launched a comprehensive effort to promote the deployment of IoT products and services to "secure [Germany's] technological leadership role and establish itself as an [IoT] lead market and provider."[30] Again, however, these should be industry led efforts, not mandated by government regulators; as the development of the IoT to date has shown, industry will be best positioned to create a uniform international, interoperable framework.

D. THE POLICY FRAMEWORK SHOULD PROMOTE THE INCREASED AVAILABILITY AND EFFICIENT USE OF SPECTRUM.

The projected number of IoT devices will place additional demands on spectrum resources, requiring a continued growth in spectrum available for general commercial use, both licensed and unlicensed. Even if just ten percent of the total number of IoT devices were to be directly connected to commercial mobile networks (i.e., with a SIM card and on a 3G/4G/5G network), that still represents billions of new devices operating on wireless networks worldwide. Additionally, the absolute growth in, and the heterogeneity of, IoT traffic will combine with the continued growth in overall demand for mobile broadband to pressure licensed spectrum resources. Similarly, a very high portion of those devices that are *not* directly connected to commercial mobile networks—though they may be indirectly connected via gateway devices that are on a commercial mobile network—will be using unlicensed or non-commercially allocated spectrum.

However, there is no need for governments to allocate dedicated spectrum specifically for IoT or IoT segments. NTIA, Congress, and the FCC should continue efforts to find and

---

[30] *See, e.g., Industrie 4.0, Smart Manufacturing for the Future*, Germany Trade and Invest (describing a comprehensive blueprint for the German government, industry and other stakeholder for fostering the development of IoT products and services), *available at* http://www.gtai.de/GTAI/Content/EN/Invest/_SharedDocs/Downloads/GTAI/Brochures/Industries/industrie4.0-smart-manufacturing-for-the-future-en.pdf.

reallocate spectrum for commercial mobile broadband use. Provided that sufficient licensed spectrum is allocated for mobile broadband use, there is no reason to expect that dedicated spectrum to support IoT devices should be needed: it should be left up to spectrum licensees to manage and employ their spectrum in an optimized fashion for the mix of traffic types that may be simultaneously using licensed bands. The federal government should also continue to support the progress being made by industry standards bodies in the development of new standards, and work toward international harmonization of spectrum allocations where appropriate.

E. GOVERNMENTS CAN TAKE STEPS WITH RESPECT TO THEIR OWN ACTIONS, FACILITIES AND ACQUISITIONS TO SUPPORT THE DEPLOYMENT AND ADOPTION OF IOT SOLUTIONS.

AT&T noted in Section II.C. of these Comments that the Government plays other roles in the IoT ecosystem beyond those of regulator or enforcer. In particular, the Government acts as an Influencer, as a Funder/Facilitator, and as a Customer. Each of these roles comes into play in establishing a sound and comprehensive policy framework for the IoT, as policymakers at all levels of the country's governments can also accelerate the deployment and adoption of IoT solutions.

1. Government Actions as an Influencer.

As noted above, there are already examples where government agencies have constructively served in a helpful capacity as a convener of multi-stakeholder processes addressing specific IoT issues or concerns. For the right issues and with the right participants, there are likely to be opportunities for similarly productive endeavors in the future. Similarly, many government organizations—such as the GAO, NIST, FTC, and NTIA itself, to name but a

few—are likely (or required) to produce reports on IoT related topics.[31] The lens through which each of these agencies views and discusses the IoT will influence subsequent stakeholder thinking about the IoT, whether internal to the government, in the public, or among industry players. Here again, the DOC can help establish a common starting point for these kinds of reports and similar actions, to aid in achieving a coordinated and coherent view of the IoT across the government.

2. Government Actions as a Funder/Facilitator.

Governments are already directly and indirectly funding some IoT solutions deployments. The Department of Transportation, for example, is directly promoting the deployment of smart cities technologies through the $40 million it will award to the winning city of its Smart Cities Challenge.[32] It may also indirectly fund transportation management IoT solutions through a variety of programs authorized by the recently enacted FAST Act,[33] for which Congress appropriated $337 million over FY16-20. As those grants will be made to state and local governments and other organizations, the program structure and grant requirements that DoT establishes as the funder will significantly affect how any IoT solutions are brought forth from this and other programs.

---

[31] The FAST Act requires no fewer than five reports to be produced that may be germane to the IoT (*see* sections 3024, 6004, 6025, 6027, and 24113).

[32] *See* https://www.transportation.gov/smartcity.

[33] For example, section 6004 of the FAST Act directs the Secretary of Transportation to "establish an advanced transportation and congestion management technologies deployment initiative to provide grants to eligible entities to develop model deployment sites for large scale installation and operation of advanced transportation technologies to improve safety, efficiency, system performance, and infrastructure return on investment."

The federal government can and should continue to fund pilot programs and challenge grants, as both NIST and DOT are doing in their respective initiatives. These kinds of programs can provide a helpful kick start towards development and adoption, and produce valuable learnings for the private sector and governments alike.

The federal government can also speed deployment of the many network end points that will be needed for broad 5G service and denser mobile networks by facilitating deployment on Federal lands and by lowering the barriers presented by state and municipal rules. Similarly, federal agencies should coordinate and streamline the processes for applying and obtaining approval for siting wireless infrastructure on federal properties. Agencies should adopt a common set of procedures and fee schedules and ensure that those processes are applied consistently and expeditiously at individual military bases and other federal properties. NTIA's Broadband Opportunity Council has started work on some of these issues.[34]

Governments can further facilitate a more rapid deployment of IoT, particularly in the areas of smart cities and transportation, by encouraging the incorporation of IoT and networking technologies into public works and infrastructure projects, and by enabling access to public data through APIs and IoT platforms.

3. Government Actions as a Customer.

Finally, in its role as a significant customer for IoT services and products, government adoption of the IoT can be improved through continued efforts to simplify and streamline government purchasing, and coordinating between policy-making and acquisitions components

---

[34] *See* https://www.ntia.doc.gov/category/broadband-opportunity-council. AT&T filed extensive comments, available here, with the Broadband Opportunity Council, laying out at greater length its recommendations for how the federal government can spur network deployment.

of governments. Doing so will result in governments (and thus taxpayers) reaping the same sorts of transformative benefits in business processes and efficiency that so many sectors of industry are seeing from IoT adoption.

The promise of IoT for enhancing the efficient delivery of government services is profound. IoT fleet and asset management technologies can produce operational savings for many government agencies that operate large vehicular fleets or that engage in frequent shipments of goods, such as the Department of Defense. Similarly, IoT solutions, from smart thermostats and smart grid solutions to security services enabled by IoT capabilities, are beneficial to any government entity—the GSA comes immediately to mind—that manage facilities. IoT medical devices can reduce healthcare costs, benefitting the government as a major payer for (e.g., Medicare) and provider of (e.g., the Department of Veterans Affairs) healthcare. In these and many other areas of the IoT, the government is not yet well equipped to purchase IoT solutions for itself. Increasing the flexibility and adaptability of its acquisition processes to incorporate the purchase of IoT services will help foster more rapid adoption across the economy.

IV. AT&T'S RESPONSES TO SPECIFIC QUESTIONS

In the discussion above, we have sought to address many of the issues undergirding the questions posed in NTIA's request. In addition to those foregoing comments, we address below several of the specific questions posed in the Request for Comments.

RFC 1. ARE THE CHALLENGES AND OPPORTUNITIES ARISING FROM IOT SIMILAR TO THOSE THAT GOVERNMENTS AND SOCIETIES HAVE PREVIOUSLY ADDRESSED WITH EXISTING TECHNOLOGIES, OR ARE THEY DIFFERENT, AND IF SO, HOW?

Response: The opportunities arising from the IoT frequently involve the amplification and extension of the benefits that network technology and the Internet have already brought to

consumers and industry. For example, increased operational efficiency, increased consumer convenience and safety, generation of and easy access to large quantities of data, and improved insights from the analysis of that data are all benefits and opportunities that the Internet in general has provided, and that the IoT promises to apply to new areas and capabilities.

The same holds true for the challenges posed by the IoT. For example, the IoT clearly highlights concerns about privacy and security. It also presents challenges relating to the changing nature of the modern workforce and the increasing demand for highly skilled employees, particularly in the STEM disciplines.[35]

a. What are the novel technological challenges presented by IoT relative to existing technological infrastructure and devices, if any? What makes them novel?

Response: With the IoT, so many new 'elements of the physical world' ("things") have, for the first time, a significant nexus or integration with modern computing and networking technologies—both hardware and software. This means that companies that are producing these "things" must adopt and master new technologies, and that end-users—both consumers and businesses—also must gain a new understanding of the capabilities and limitations of these devices that will proliferate in their daily lives. These unique technological challenges present themselves in connection with the IoT devices themselves, the networks that connect them, and the software and platforms that support them.

- *Device challenges*: IoT devices can range from tiny—even body-implantable—beacons to major capital equipment, and from effectively disposable items to durable goods. They have widely varying requirements for power, network access, and levels of computing capability. They may be constantly in contact with a person, or installed in a remote location largely inaccessible to people.

[35] *See, e.g.*, http://www.business.att.com/content/whitepaper/idc-developers-iot-playbook.pdf.

- *Network challenges:* The novel network challenges associated with the IoT include support for the wide number and diversity of IoT devices and the traffic they generate (both payload and signaling), the need for ubiquitous coverage, and the need for global operability. In particular, the IoT creates the imperative for denser, higher-speed, scalable, dynamic, secure and ubiquitous networks. This has major ramifications for spectrum resources and the deployment of network infrastructure.
- *Software / platform challenges:* These include the need to develop expertise and experience among the developers who are creating IoT applications. In addition, providers must deal with new Big Data and analytics challenges, as they must work through the massive amounts of data generated from the huge number of diverse IoT devices to deliver their services and products efficiently.

b. What are the novel policy challenges presented by IoT relative to existing technology policy issues, if any? Why are they novel? Can existing policies and policy approaches address these new challenges, and if not, why?

Response: The combination of the cross-sector and cross-jurisdictional nature of IoT use cases and business models with the interaction between cyber and physical systems means that policymakers are encountering new policy issues, new stakeholders, and new technologies with which they may not be familiar. As described earlier in these comments, the policy issues facing regulators may have both vertical and horizontal components, with effects implicating the jurisdictions of many different governmental entities. Thus, policy makers must now recognize that they cannot necessarily act in their traditional silos, or expect that the effects of their policies will be isolated to their traditional areas. They instead must be cognizant that policies applied in one area may well spill over to areas outside of their jurisdiction—and incorporate that perspective, and corresponding coordination, into their policymaking activities.

c. What are the most significant new opportunities and/or benefits created by IoT, be they technological, policy, or economic?

Response: The opportunities and potential benefits of IoT extend to all areas of the economy, society and government. For businesses, the IoT will provide the opportunity to

generate greater efficiency and intelligence in business operations. The combination of IoT technologies and data analytics also will provide companies with unprecedented insight into their operations, and will significantly improve their ability to serve their customers. For those customers, in turn, the IoT will mean increased convenience and control of their lives and their environments. This extends to the government as a customer for IoT solutions as well; as with private businesses, IoT technologies will improve government's insight into, and ability to deliver, services to their constituents. IoT solutions also provide the means for governments at all levels to move toward many policy objectives, such as increased energy and water efficiency, improvements in public health, increased automotive safety, and better infrastructure management.

RFC 2 **THE TERM "INTERNET OF THINGS" AND RELATED CONCEPTS HAVE BEEN DEFINED BY MULTIPLE ORGANIZATIONS, INCLUDING PARTS OF THE U.S. GOVERNMENT SUCH AS NIST AND THE FTC, THROUGH POLICY BRIEFS AND REFERENCE ARCHITECTURES. WHAT DEFINITION(S) SHOULD WE USE IN EXAMINING THE IOT LANDSCAPE AND WHY? WHAT IS AT STAKE IN THE DIFFERENCES BETWEEN DEFINITIONS OF IOT? WHAT ARE THE STRENGTHS AND LIMITATIONS, IF ANY, ASSOCIATED WITH THESE DEFINITIONS?**

Response: Given the still nascent and evolving nature of the IoT, it is both premature and counterproductive to attempt to define it. Indeed, the evolving nature of the IoT makes a clear definition impracticable. The DOC's resources are better spent describing IoT technologies and use cases, and then monitoring their deployment.

In particular, AT&T is concerned that creating a definition of IoT technology is the first step toward prescriptive regulation. Once such a definition exists, the focus turns to whether a particular application falls within, or outside of, the definition, almost inevitably with some regulatory consequences.

RFC 3 WITH RESPECT TO CURRENT OR PLANNED LAWS, REGULATIONS, AND/OR POLICIES THAT APPLY TO IOT:

a. Are there examples that, in your view, foster IoT development and deployment, while also providing an appropriate level of protection to workers, consumers, patients, and/or other users of IoT technologies?

Response: Yes, as described in our Comments there are several notable examples of existing programs that already foster IoT development, and that serve as useful models for future initiatives. For example, challenge type programs, such as NIST's Global Cities Team Challenge and DoT's Smart Cities Challenge, help spur the deployment and adoption of IoT solutions. Similarly, the FAST Act, as discussed above, is an example of legislation that enabled funding for technology deployment within the context of surface transportation infrastructure construction and maintenance.

b. Are there examples that, in your view, unnecessarily inhibit IoT development and deployment?

Response: Unfortunately, there are several recent examples of actions at the federal level that threaten the development of the IoT marketplace. A prime case in point is the FCC's proposed rule imposing new and asymmetrical privacy rules on Internet Service Providers. The FCC's action not only directly impacts a cross-sectoral issue—privacy—intruding on and supplanting another agency (the FTC) that has extensive and long-running expertise in the area, but it does so in a way that creates customer confusion, disserves the interests of privacy and innovation, disadvantages one segment within the IoT relative to another and inhibits the ability of companies to deploy IoT solutions.

RFC 4 **ARE THERE WAYS TO DIVIDE OR CLASSIFY THE IOT LANDSCAPE TO IMPROVE THE PRECISION WITH WHICH PUBLIC POLICY ISSUES ARE DISCUSSED? IF SO, WHAT ARE THEY, AND WHAT ARE THE BENEFITS OR LIMITATIONS OF USING SUCH CLASSIFICATIONS? EXAMPLES OF POSSIBLE CLASSIFICATIONS OF IOT COULD INCLUDE: CONSUMER VS. INDUSTRIAL; PUBLIC VS. PRIVATE; DEVICE-TO-DEVICE VS. HUMAN INTERFACING.**

Response: See the discussion in Section II of these comments concerning a common conceptual and definitional framework for the IoT.

RFC 8 **HOW WILL IOT PLACE DEMANDS ON EXISTING INFRASTRUCTURE ARCHITECTURES, BUSINESS MODELS, OR STABILITY?**

Response: One key role for IoT is in better monitoring and assessing existing physical infrastructure, such as for transportation (bridge, roads, ports, rail lines) and utilities (water lines, electrical facilities). IoT technologies offer significant benefits in all of these areas, holding the promise to allow governments to more effectively target their infrastructure spending and better avoid the dangers that attend infrastructure failures.

As for the communications infrastructure that supports the IoT, the IoT will reinforce growing demand for increased bandwidth and increased coverage provided by network facilities. This will serve as continued stimulus for private sector investment—so long as governments do not create disincentives for that investment—as well as a hastened transition to an all-IP infrastructure.

There are synergies available here: the physical infrastructure investments that incorporate or adopt IoT capabilities may well enable new opportunities for network infrastructure deployment. Similarly, expanded or deepened network deployments can open up new areas of viability for physical infrastructure adoption of IoT.

RFC 15 WHAT ARE THE MAIN POLICY ISSUES THAT AFFECT OR ARE AFFECTED BY IOT? HOW SHOULD THE GOVERNMENT ADDRESS OR RESPOND TO THESE ISSUES?

Response: As AT&T has discussed in these Comments, it is critical that the Government—preferably under the leadership of the DOC—develop a National policy framework for IoT that can help ensure the on-going, robust network deployment necessary to support this technology into the future. The Government's policies must provide for a unified national framework for the IoT, minimize regulatory burdens, and provide policy certainty that will create the climate to maximize essential infrastructure investment. The key attributes of that Framework should include:

- Support for the collaborative, self-regulatory initiatives among industry stakeholders that have fueled the growth of the IoT to date.
- In those limited cases where regulatory action may be justified, use of a light touch, flexible, well-coordinated regime that protects innovation and facilitates rapid IoT market developments.
- An international interoperable policy framework for IoT that facilitates the seamless global deployment of IoT products and services.
- Progressive spectrum policies that promote the robust allocation of additional spectrum and the progress being made by industry and the standards bodies.

RFC 16 HOW SHOULD THE GOVERNMENT ADDRESS OR RESPOND TO CYBERSECURITY CONCERNS ABOUT IOT?

Response: See the discussion in Section III.B.1 of these Comments. As AT&T details there, the Government should refrain from any prescriptive regulation in the area of cybersecurity, as such measures would have a counter-productive effect on stakeholders' ability to respond to ever-changing threats. Instead, in all cases in the United States the NIST Cybersecurity Framework should be the starting point on all security questions related to the IoT.

RFC 17 HOW SHOULD THE GOVERNMENT ADDRESS OR RESPOND TO PRIVACY CONCERNS ABOUT IOT?

Response: See the discussion in Section III.B.2 of these Comments. As AT&T describes there, many IoT applications do not involve personally identifiable data and consequently present no meaningful privacy risk. Nevertheless, to the extent intervention is necessary, the FTC is the country's expert agency on privacy. The FTC should be tasked with ensuring appropriate privacy protections for the IoT and should proceed, as it typically does, through enforcement across the sector, rather than through ex ante rule-making. And industry should continue as it has in being proactively engaged in voluntary and collaborative processes to provide appropriate privacy protections for IoT applications.

RFC 21 WHAT ISSUES, IF ANY, REGARDING IOT SHOULD THE DEPARTMENT FOCUS ON THROUGH INTERNATIONAL ENGAGEMENT?

Response: As AT&T has noted, the Department of Commerce has a vital role to play in advocating for international policies that avoid unnecessary burdens on global IoT applications.[36] The policy framework for international engagement must protect cross-border data flows and avoid localized data retention requirements. Regulators also must allow IoT

[36] *See supra*, Note 30 (citing *Industrie 4.0.,* Germany Trade and Invest).

providers to choose between various available options for numbering and device management, rather than imposing a single, one-size alternative for all cases. And as with domestic regulatory policy, the DOC should encourage international governments to promote the development of standards and operating frameworks for IoT that are industry led, voluntary processes.

RFC 26 WHAT ROLE SHOULD THE DEPARTMENT OF COMMERCE PLAY WITHIN THE FEDERAL GOVERNMENT IN HELPING TO ADDRESS THE CHALLENGES AND OPPORTUNITIES OF IOT? HOW CAN THE DEPARTMENT OF COMMERCE BEST COLLABORATE WITH STAKEHOLDERS ON IOT MATTERS?

Response: As AT&T has described throughout these Comments, the Department of Commerce is uniquely positioned to establish a leadership position on IoT policy within the Federal government, and to use that position—informed by the results of this Request for Comments—to work with stakeholders across the ecosystem, both within the United States and internationally, to establish a comprehensive, coherent, and consistent policy framework that will promote the continued development of IoT worldwide. In particular, the DOC/NTIA should use its leadership position on IoT issues to consider launching an interagency process designed to align and harmonize regulatory actions affecting the IoT so as to promote a National policy framework that can help ensure the on-going, robust network deployment necessary to support IoT technology into the future.

CONCLUSION

AT&T applauds the DOC and NTIA for undertaking this important inquiry into the potential role of Government in the development of IoT. The continued robust deployment of the IoT will hinge on the establishment of policies that enable the massive private investment in mobile networks that is the sine qua non of the IoT ecosystem. The DOC and NTIA are particularly well-positioned to take a leadership role in developing a national policy framework that will support that investment and deliver the promise of the IoT for all Americans. AT&T looks forward to continue working with the DOC and NTIA in that important work.

Respectfully submitted,

/s/ *Robert C. Barber*
Robert C. Barber
James Wade
David Lawson
AT&T Services, Inc.
1120 20th Street NW
Suite 800
Washington, D.C. 20036
(202) 457-2121 (phone)

June 2, 2016