BEFORE
THE 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 INTERNET2

John S. Morabito
Danielle N. Rodier
Internet2
1150 18th Street, NW
Suite 900
Washington, DC 20036

Alan G. Fishel
Adam D. Bowser
Arent Fox LLP
1717 K Street NW
Washington, DC 20036
Counsel for Internet2

Dated: June 2, 2016

Table of Contents

Page

I. Introduction

The University Corporation for Advanced Internet Development (d/b/a "Internet2") submits these comments in response to the Notice and Request for Public Comment ("Notice") issued by the National Telecommunications and Information Administration ("NTIA") regarding the benefits, challenges, and potential roles for the government in fostering the advancement of the Internet of Things ("IoT").[1]

The research and education ("R&E") community is in a unique position to comment on IoT, because it will act as both a testbed for innovation and standards, in partnership with funding agencies and the private sector, and a consumer of IoT technologies in the context of developing Smart Campuses. Accordingly, Internet2 encourages NTIA to incorporate the views of the R&E community in this proceeding.

II. Executive Summary

The Internet as it exists today is designed and optimized largely for top-down traffic flows, where a few very large content providers asymmetrically distribute data downstream to consumers. IoT, by contrast, is an entirely different construct, with decentralized networked devices creating and pushing content to compute-and-storage resources in the cloud to provide actionable intelligence for decision makers, or, indeed, systems designed to make decisions themselves. Given the novel technological and policy issues created by the increased prevalence of connected devices in our environment, Internet2 respectfully submits that Internet2 and the R&E community as a whole are well positioned to assist NTIA and other policymakers address the benefits and challenges of IoT. In these comments, Internet2 focuses on the following five aspects of IoT and related policy.

---

[1] Available at https://www.ntia.doc.gov/files/ntia/publications/fr_rfc_iot_04062016.pdf ("Notice").

First, policymakers should define IoT in terms of the continued diffusion and integration of information technology into interconnected systems. We cannot lose sight that the "things" in IoT are part of larger systems that need to be viewed holistically in order to truly assess the benefits and challenges presented by the growth of connected devices.

Second, the growth of IoT will require targeted and forward-looking approaches to U.S. broadband policies that promote the deployment of high-capacity networks optimized for symmetrical traffic demand and support the increased availability of spectrum.

Third, to truly unlock the potential of IoT, disparate devices and systems will need to communicate with each other. Policymakers therefore should encourage open standards and the adoption of IPv6 to assign IP addresses.

Fourth, policymakers should look to the current research activities being conducted within the R&E community, including Internet2's own IoT Working Group, to help them learn more about IoT developments.

Finally, given that the increased deployment of connected devices and more intelligent systems will bring about many challenges for both individuals and businesses, Internet2 recommends that stakeholders should address Trust, Identity, Privacy, Protection, Safety, and Security ("TIPPSS") during the development of any IoT application.

III. Background

A. Internet2

Internet2 is a member-owned, not-for-profit corporation founded in 1996 by the nation's leading higher education institutions. Today, Internet2 has grown to more than 503 members, including at least 317 research universities, government agencies and laboratories, private companies, and regional networks that provide advanced networking to a wide range of universities, government agencies, and community anchor institutions ("CAIs"). Through its

position as the country's premier national research and education network ("NREN"), Internet2 promotes the next-generation R&E missions of its members by providing pioneering network capabilities and unique opportunities for cross-collaboration to develop innovative solutions to common technology challenges, including through its IoT Working Group.

Internet2 has tremendous experience installing and managing next-generation broadband infrastructure, including having completed a $62.5 million Broadband Technology Opportunities Program ("BTOP") project. This project, funded by NTIA, helped to fulfill the recommendation of the National Broadband Plan that government agencies work with the R&E community to facilitate a "'Unified Community Anchor Network,' that would support and assist anchor institutions in obtaining and utilizing broadband connectivity."[2] Today, with this infrastructure in place, Internet2 serves as the backbone for state and regional networks that interconnect more than 93,000 CAIs throughout the country.[3]

Internet2 owns and operates a premier advanced national network infrastructure and identity management framework that serves a variety of constituencies within the R&E community. Using the latest generation of optical transport equipment, the Internet2 Network supports native 100 Gigabit services with near-term potential of offering 200 and 400 Gigabit services. Additionally, the Internet2 Network has advanced Layer 2 services built on software defined networking ("SDN"), which allows users to optimize the network for their specific application needs.[4] Internet2's current 8.8 Terabit capacity national network positions the

---

[2] *Connecting America: The National Broadband Plan* at 154 (Rel. Mar. 16, 2010) ("NBP") available at http://www.broadband.gov/plan.

[3] Internet2's U.S. Unified Community Anchor Network program ("U.S. UCAN"), the outgrowth of its BTOP award, focuses on extending R&E network resources to all CAIs, thereby expanding access to, and ultimately adoption of, next-generation broadband.

[4] Internet2 has deployed the world's first SDN-based 100G network to reopen innovation in networking and ensure continued global leadership in the development of next-generation

Internet2 Network as one of the most advanced networks in the world. Internet2 has built its business models to encourage advanced applications to use bandwidth, eliminating per-unit billing systems in favor of investing in capacity in advance of demand. Internet2 also helps the R&E community select, develop, and deliver its own cloud and trust solutions through the Internet2 NET+ program with commercial cloud service providers, maximizing the benefits of collaborative cloud environments and scale for academic institutions.

Internet2's collaboration is extended not only by deep relationships with dozens of state and regional networks in the U.S. but also mission-driven networks in leading science agencies, such as the Department of Energy's Energy Sciences Network ("ESnet") and the National Oceanic and Atmospheric Administration's science network, N-Wave. Internet2 also collaborates with federal agencies by providing network and membership services to the Department of Agriculture, National Institute of Standards and Technology ("NIST"), Centers for Disease Control and Prevention, National Institutes of Health, the National Park Service, and other federal agencies.

In addition, Internet2 has played an integral role in the shift toward global R&E collaboration, which has necessitated a fundamental change in how scientists and network providers interact.[5] The global information-age economy was born from the substantial investments in R&E here in the U.S., and Internet2 continues to play an active role in expanding

---

network technologies. This investment supports programs like the National Science Foundation Global Environment for Networking Innovations ("GENI") project and also provides a nationwide cyber-instrument to support scientists with data-intensive networking needs in the campus environment.

[5] As one example relevant to IoT developments, the Large Hadron Collider ("LHC") creates massive amounts of raw detector data that must be moved, stored, and processed in accordance with a highly distributed computing model. Internet2 worked with ESnet and US LHCNet, which provides transatlantic network connectivity from the LHC facility, to deploy networks with the bandwidth and capabilities to reliably transport multiple streams of 10 Gigabits of data per second.

the reach of its R&E members on a global scale. In fact, Internet2 has relationships with more than 65 foreign regional networks. These relationships include peering agreements to exchange traffic, with the goal of advancing science, networking, and cooperation between the foreign regional networks and user communities they serve.

B. The R&E Community and IoT

As with many new technological breakthroughs, IoT's roots can be traced back to the R&E community. In 1999, computer scientists from the Massachusetts Institute of Technology and six other research universities were working in the field of networked radio frequency identification ("RFID") and emerging sensor technologies.[6] Since this time, when the R&E community first connected devices to a network for a particular application, IoT has witnessed exponential growth, with billions of connected devices today across an ever-increasing diversity of applications, networks, and devices.

As IoT expands, so does our interaction with systems that can silently collect, process, create, and act on information that we generate, individually and collectively, as we conduct our lives. IoT represents a computing system where the data *is* our environment, including the people who live in it. This requires new approaches that span everything from security to privacy.

As indicated in the Notice, the number of networked devices was estimated to be about 25 billion last year, and it is predicted that the number of connected devices will grow to 200 billion by 2020.[7] The incredible amount of devices that will be connected to the Internet will create massive demands on broadband networks. Because the Internet2 Network, along with the networks of its state and regional networking partners, already is catering to the demands of the

---

6 *See* http://postscapes.com/internet-of-things-history.

7 *See* Notice n.2.

most intensive data users from both a quantitative and qualitative perspective, Internet2 is uniquely capable of meeting the forecasted network demands of IoT applications.

The growth of IoT will challenge us technologically because it will upend the current network traffic paradigm. Today's Internet is optimized to distribute data from a few content providers to a large number of consumers. This means that the Internet is architected and engineered to accommodate mostly downstream data flows, and is further optimized to deliver the same content (e.g., a particular Netflix movie) to a large number of users.

By contrast, IoT, consisting of more and more data coming from more and more things, will turn the status quo on its head by requiring a network architecture optimized for many widely distributed content providers (i.e., sensors) sending their raw data to compute-and-storage resources for aggregation, knowledge creation, and action. Moreover, network resiliency and availability (i.e., network uptime) will become increasingly important as more and more everyday devices become connected to the Internet and rely on it to function. For example, if a home security system or even a hallway light switch cannot function without broadband and cloud processing, it is imperative to implement network engineering and management policies that encourage providers to increase network uptime standards.

IoT thus will require a network that has abundant symmetrical capacity, is not designed for predetermined traffic patterns, and is always on. The Internet2 Network is an example of just such a network on a national backbone scale, providing an incredibly high-capacity, symmetrical design to support the unpredictable patterns that the new and innovative applications generated by IoT will require.

IV. Discussion

A. Policymakers Should Define IoT In Terms Of The Diffusion Of Information Technology

IoT represents the further diffusion and integration of network-connected information technology ("IT") into our environment.[8] It is an emerging awareness that our physical surroundings increasingly are becoming part of interconnected systems. These systems may be composed of cloud-based intelligence, network connectivity, and devices embedded in our environment. This continuous digitization of our environment raises a host of ethical, privacy, and transparency challenges in terms of how individuals choose to interact with the connected devices surrounding them, including artificially intelligent devices. The "thing" in IoT is one element to classify, but these "things" are part of larger "systems" that require classification and definition in order to inform policies that nurture the development of IoT technologies holistically.

Indeed, to the extent that IT improves the human condition and protects and sustains our environment, IoT almost certainly will play a determining role in the years ahead. We no longer will imagine the application of technology without including some component of network connectivity. IoT is the modern equivalent of the 20th century's electrification. In fact, IoT has been projected to create up to $11 trillion a year in economic value by 2025, through smart cities, homes, healthcare, manufacturing, vehicles, agriculture, supply chains, retail, and offices.[9] These initiatives all will create new economic opportunities for devices, services, and process improvements that will transcend traditional regulatory silos.

---

[8] In this section, Internet2 responds primarily to Questions 1.b, 1.c, and 2 contained in the Notice.

[9] *See* http://www.mckinsey.com/mgi/overview/in-the-news/by-2025-internet-of-things-applications-could-have-11-trillion-impact.

As one example, consider the implications of a cloud-connected system that controls lighting within a building hallway. The motion sensors and the computer-controlled light switches could be classified as part of IoT. But every component, from the cloud to the sensors and light switches, is required for the system to function. The system provides both the value (lower electric bills) and the risks (privacy and increased security requirements). IoT and the systems and processes that it works through therefore require a holistic approach to the IoT landscape, related architectures, and policies, including meaningful approaches to security and safety, that will require coordination among multiple agencies and stakeholders.

While existing policies remain germane, they may not adequately address an IoT-enabled environment. IoT records our movements in the park, diagnoses our physical and mental ailments, and predicts our daily routines and habits by sharing data over the Internet in a manner that has no parallel. Future policies will need to meet the challenges that IoT presents at the intersection of privacy, safety, evolving culture, and the transformative benefits it can bring. The revolutionary changes that IoT will bring in terms of distributed connectedness across industries will require a new strategic approach.

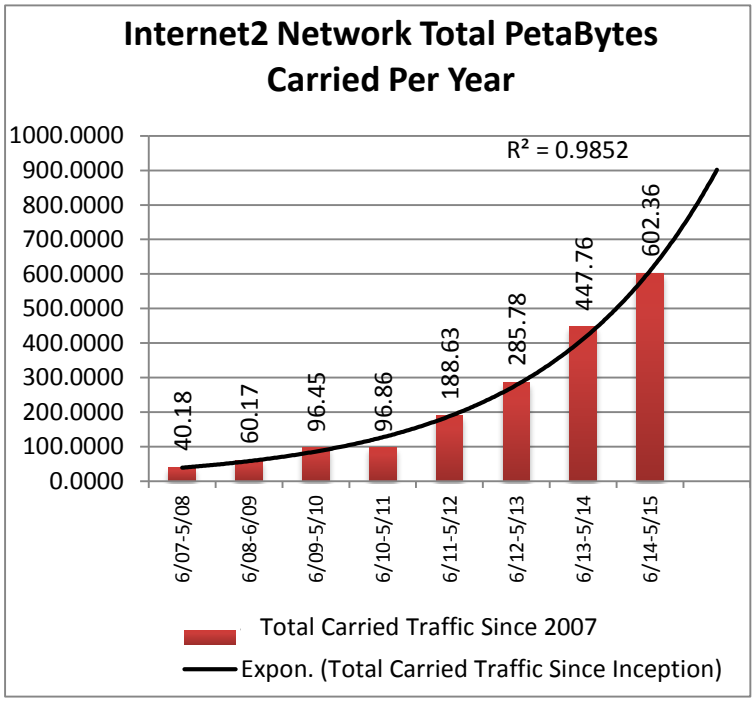
B. Broadband Abundance And Spectrum Management Will Help To Address The Technology Challenges And Opportunities That IoT Presents

IoT encompasses an ever-growing cycle of innovation enabled by a wide range of technologies and applications.[10] At its core, however, IoT is supported by evolving and expanding wireless and wired communications networks and broadband infrastructures that are used to manage and transport data between devices in a diffuse environment. The anticipated traffic flows resulting from the growth of connected devices will differ dramatically from how the Internet currently is architected, and new policies will need to be developed to optimize

[10] In this section, Internet2 responds primarily to Questions 1.a and 8 contained in the Notice.

network resiliency and availability to meet this new paradigm. Given the exponential growth of connected devices and the corresponding exponential growth in symmetrical broadband usage resulting from IoT devices, the deployment of future-proof broadband in advance of demand and spectrum management now are more critical than ever.

As Federal Communications Commission Chairman Wheeler recently stated, "a wireless network is mostly wired."[11] As the operator of one of the world's most advanced broadband networks, Internet2 knows that rapid advancements in both networking technologies and the applications that run over those networks quickly can and do make what would appear to be a high-capacity broadband connection today less than adequate in the near future.



Indeed, Internet usage has a consistent pattern of doubling traffic approximately every one to two years. Policymakers therefore must support broadband abundance policies and technologies that cost-effectively expand to enable growing demand and ensure that broadband capacity does not become the bottleneck of IoT evolution and growth.

The users of R&E networks, like the one operated by Internet2 and its state and regional networking partners, are some of the most demanding Internet users in the country, such as

[11] *See* http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db0502/FCC-16-54A2.pdf.

scientists, academics, and researchers in some of the nation's leading institutions. They have expectations that they can symmetrically move massive amounts of data on demand, that the network will deliver a predictable throughput at all times they offer a workload to the network, and that their network service providers will continuously expand the network to stay slightly ahead of the demand they are likely to generate. The R&E community has had tremendous success operating networks that not only meet those needs today but also serve as the necessary testing grounds for the applications of tomorrow.[12] Internet2 and its state and regional networking partners therefore have a wealth of experience developing best practices that NTIA and other policymakers can leverage to facilitate the deployment of high-capacity broadband that will be future proof and capable of facing the unique challenges posed by IoT broadband infrastructure requirements.

In addition, IoT relies on all forms of wireless communication, including unlicensed Wi-Fi, licensed cellular/mobile, free space wireless, infrared, and ultrasonic communication. Given the physical constraints of spectrum, especially spectrum with desirable propagation traits, the success of IoT's ability to improve the human condition also depends on effective spectrum management. Coordinated availability of reliable spectrum is IoT's oxygen. Further, while the future applications of IoT are emerging, it is likely that many will present demands for ubiquitous high throughput and mobile connectivity in a variety of environments. Spectrum availability therefore will be a key requirement due to the distributed compute, storage, cloud, and collaboration resources required by IoT applications.

[12] Internet2, through its U.S. UCAN program, has partnered with nonprofit organization US Ignite on its Sustainable Ecosystem of Smart Applications project. Internet2 will support the deployment and adoption of gigabit applications among CAIs in at least 15 cities, thus creating an "application test bed" community of CAIs.

C. Open Standards And Collaboration Are Critical To The Success Of IoT Development

IoT as we know it today is made up of a loose collection of disparate, purpose-built networks and connected devices.[13] To truly unlock the potential of IoT, it will be necessary for disparate IoT systems to communicate with one another. Open standards therefore are critical in combining a wide range of data sets across myriad environments and applications. Conversely, the advances of IoT could be impeded unnecessarily by proprietary data standards. NTIA and other agencies therefore should promote open standards consistent with these comments, particularly regarding the universal deployment of IPv6.

IPv6 is the most recent version of the protocol that is used to assign IP addresses, which are the unique numbers assigned to connected devices. Today's Internet, however, primarily relies on an outdated version of the Internet Protocol (IP), known as IP version 4 (IPv4), which assigns 32-bit addresses. This means that IPv4 has the capacity to assign approximately 4.3 billion unique IP addresses (or 2 the 32nd power). In other words, due to the rapid increase in the number of interconnected devices that use IP addresses, we already have exhausted the limitations of IPv4, which ran out of addresses more than five years ago. The continued use of IPv4 therefore severely restricts the number of devices that can be connected to the Internet.

The solution to this problem lies with IPv6, which assigns 128-bit addresses and thus has the capacity to assign 340 trillion trillion trillion addresses (or 2 to the 128th power). This means that for the foreseeable future, there is now an effectively limitless quantity of unique IP addresses available to identify new devices. This is particularly important in the context of IoT deployment because every device that connects to the Internet can have its own unique, persistent identifier without the need for local networks to share IP addresses, which would

[13] In this section, Internet2 responds primarily to Question 6 contained in the Notice.

otherwise decrease the usefulness of IoT-driven data innovation. Indeed, IoT systems will capture, analyze, and act on data at an unprecedented scale, and components of these systems will require very high-speed networks, as well as advanced network services such as network segmentation, IPv6, and deterministic latency.

Networks that serve the global R&E community have deployed IPv6 pervasively for the last 20 years. In fact, the Internet2 Network and the networks of its state and regional networking partners connected to university campuses and national lab facilities represent the single largest contiguous deployment of IPv6. The R&E community is thus an ideal national-scale testbed for these advanced services where the challenge of ensuring that IoT technologies and systems can communicate well across a standard open architecture can be addressed.

Further, there are multiple standards efforts being conducted by entities such as the Internet Engineering Task Force ("IETF"), Industrial Internet Consortium ("IIC"), and NIST. These efforts need to be correlated to ensure safe, secure, low latency communications to support IoT systems, applications, and services. Internet2 respectfully submits that NTIA and other policymakers should therefore look to the R&E community to facilitate the coalescence around open standards that can work for all IoT stakeholders.

D. Policymakers Should Consider Current Research Initiatives Being Conducted Within The R&E Community

NTIA seeks information on any current or recent initiatives "that have examined or made important strides in understanding the IoT policy landscape."[14] Internet2 submits that the following initiatives may be of interest to NTIA in this regard:

- The Institute of Electrical and Electronics Engineers ("IEEE") has held a series of "Experts in Technology And Policy" forums, which have identified several policy issues and

[14] Notice, Question 5.

related technology implications regarding the Internet and IoT. Internet2, IEEE, and the National Science Foundation ("NSF") also co-sponsored a workshop on End-to-End Trust and Security for IoT at which the participants developed a set of technological implications and recommendations.

- The Internet2 IoT Working Group has brought together leading IoT experts from the R&E community to work through a number of emerging issues, including using network segmentation to ensure that IoT devices do not undermine overall network security, developing recommendations for a comprehensive End-to-End Trust and Security open architecture for IoT, determining the components of IT infrastructure for IoT enablement, and creating a sandbox environment for testing and piloting by university researchers.[15]

- Last year, Google selected Carnegie Mellon University to lead a multi-university IoT expedition project, which will include creating a new platform for IoT applications, in partnership with Stanford University and the University of Illinois. Carnegie Mellon also plans to evolve its campus into a living laboratory through the large-scale deployment of IoT technology.[16]

- The University of Madison-Wisconsin has established an Internet of Things Lab for collaborations between the university and industry that foster the understanding, accelerated innovation and development, and successful deployment and adoption of IoT technologies and education.[17]

---

15 http://www.internet2.edu/communities-groups/advanced-networking-groups/internet-things-iot/.

16 https://campustechnology.com/articles/2015/07/13/carnegie-mellon-to-lead-internet-of-things-expedition.aspx.

17 http://www.iotlab.wisc.edu/default.aspx.

E. Policymakers Should Look To Trust, Identity, Privacy, Protection, Safety, and Security To Minimize Disruptions On Existing Infrastructure

IoT will profoundly change the nature of infrastructure, create new services, and increase our dependence on IT in general. The Internet already has combined with critical infrastructure, such as electrical generation and distribution, transportation, and first responder communications, to amplify its benefits and risks. The continued wave of integration will bring both additional benefits and risks to nearly every aspect of our global environment.[18]

IoT also will both disrupt and enhance business models, with the user experience in mind. Current examples include Uber disintermediating the taxi and limousine industry and Airbnb disrupting the hotel/motel industry. Traditional business models will continue to adapt, disintermediate, or develop a hybrid approach to accommodate traditional user and new user experiences.

In order to adequately address this new environment, policymakers and stakeholders should consider Trust, Identity, Privacy, Protection, Safety, and Security ("TIPPSS"). All new applications, devices, and use cases for IoT should address these needs, and policies should evolve to contemplate them, especially, for instance, in the case of connected healthcare devices or connected vehicles. The successful diffusion of IT into the environment requires substantial breakthroughs in TIPPSS.

Specifically, the "Trust" of the device and user must be addressed, e.g., it is the user we think it is, the doctor we think should be accessing the connected medical device, or the sensor we think is checking the water supply. The "Identity" of the user needs to be authenticated to ensure that it is actually the credentialed individual we believe it is. The data and individual

---

[18] IoT devices will require additional power for the digital elements added to physical devices. This will be available through batteries and connections to energy sources such as the electric grid and renewable energy sources.

"Privacy" parameters must be met and considered, such as Health Insurance Portability and Accountability Act ("HIPAA") regulations that stipulate how protected health information must be handled. We must further provide "Protection" of the data and user, such as preventing unauthorized exposure of data in a cloud environment or in an IoT device itself. The "Safety" of an individual, such as in a connected vehicle, needs to be ensured. And finally, the "Security" of the data – the critical infrastructure – must be maintained.

These breakthroughs will require a combination of basic research and effective transition to practice. Without leaps in effective TIPPSS, the next cyber incident could be kinetic and devastating. Internet2 has been working with IEEE and NSF to increase the focus on TIPPSS. The use of TIPPSS in the country's educational curriculum and in the development of all IoT devices and systems should be encouraged, and Internet2 respectfully submits that NTIA should leverage the R&E community's experience in this regard.

V. Conclusion

For all of the foregoing reasons, Internet2 respectfully requests that NTIA consider the above recommendations as it continues to develop policies regarding IoT.

Respectfully submitted,

/s/ John S. Morabito
John S. Morabito
Vice President, General Counsel, and
Corporate Secretary
Internet2
1150 18th Street, NW
Suite 900
Washington, DC 20036