

**Before the
DEPARTMENT OF COMMERCE
National Telecommunications and Information Administration
1401 Constitution Avenue, NW
Washington, D.C. 20230**

In the Matter of)	
)	
The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things)	Docket No. 160331306–6306–01 IOT RFC 2016
)	
)	
)	

**COMMENTS OF
THE UNITED STATES TELECOM ASSOCIATION**

The United States Telecom Association (USTelecom)¹ is pleased to comment on the Notice and Request for Comments (Notice) issued by the National Telecommunications and Information Administration (NTIA), U.S. Department of Commerce (Department) regarding its inquiry requesting public comment to review the current technological and policy landscape regarding the Internet of Things (IoT).² Through its Notice, NTIA seeks broad input from all interested stakeholders on the potential benefits and challenges of IoT technologies and what role, if any, the U.S. Government should play in this area.³

I. Introduction

As the nation moves towards the development and deployment of IoT technology, USTelecom’s member companies are ideal partners to facilitate the widespread deployment and

¹ USTelecom is the premier trade association representing service providers and suppliers for the telecommunications industry. USTelecom members provide a full array of services, including broadband, voice, data and video over wireline and wireless networks.

² See, Notice and Request for Comment, *The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things*, 81 FR No. 66, p. 19956 April 6, 2016 (*Notice*).

³ *Notice*, p. 19956.

adoption of such tools and services. USTelecom's member companies provide a full array of services to consumers, businesses and government agencies at the local, state and federal levels. These broadband-enabled suites of services range from traditional voice telephony, consumer broadband and video, as well as managed secure services for businesses and government agencies. Consumers and businesses alike are reaping the benefits that broadband networks afford.

USTelecom agrees with the Department's and NTIA's recognition of the "importance of the Internet to U.S. innovation, prosperity, education, and civic and cultural life." USTelecom has advocated at length on the role that the Internet economy plays in the United States, and we are encouraged that the Department has made it a top priority to encourage growth of the digital economy and to facilitate an environment that ensures continued growth and innovation within this space.

While correctly asserting that "IoT has the potential to catalyze new user applications and give rise to new industries,"⁴ the Department should be cautious about viewing IoT services as radical and transformative new technological offerings. Instead, the development and deployment of such technologies are more accurately viewed as an evolution and extension of existing Internet capabilities. Although IoT technologies and services are in their nascent stage and hold significant promise, they do not represent a technological development that warrants fundamental change to existing statutory and regulatory frameworks, and particularly should not trigger new technology-specific regulation.

⁴ *Notice*, p. 19957.

II. NTIA Should Develop a Policy Framework that Incentivizes Investment in Broadband Infrastructure.

The IoT solution will depend upon both public and private connectivity. Such connectivity will require deployment of robust broadband infrastructure for the purpose of interconnecting devices. As such, ubiquitous connectivity will be an important factor in achieving those benefits. USTelecom's member companies, many of which are small businesses, annually invest tens of billions of dollars in America deploying, improving and maintaining communications networks that make available voice, video and broadband services to virtually every home and business in this country. There are few if any industries that are more committed to supporting American economic growth through private investment in their essential infrastructure.

Broadband providers have aggressively moved towards that goal, having invested \$78 billion in network infrastructure in 2014 in the United States, according to an analysis by USTelecom.⁵ That number represents a \$3 billion, or 4 percent, increase in investment over 2013 and \$14 billion, or 22 percent, increase over 2009 investment. Yet, recent regulatory decisions by the Federal Communications Commission (FCC) have increased barriers to broadband investment and innovation.⁶ Moreover, infrastructure investment by broadband

⁵ See *Broadband Investment Gains Continued in 2014*, USTelecom Research Brief (Jul. 24, 2015) (available at <http://www.ustelecom.org/sites/default/files/documents/Investment-2014-Research-Brief-July-2015.pdf>).

⁶ See, e.g., *Protecting and Promoting the Open Internet*, Report and Order on Remand, Declaratory Ruling, and Order, GN Docket No. 14-28, 30 FCC Rcd 5601 (rel. Mar. 12, 2015) (defining all Internet access services as telecommunications services and subjecting them to burdensome, public utility-style regulations); *Technology Transitions, Policies and Rules Governing Retirement of Copper Loops by Incumbent Local Exchange Carriers, Special Access for Price Cap Local Exchange Carriers, AT&T Corporation Petition for Rulemaking to Reform Regulation of Incumbent Local Exchange Carrier Rates for Interstate Special Access Services*, Report and Order, Order on Reconsideration, and Further Notice of Proposed Rulemaking, GN Docket No. 13-5, RM-11358, WC Docket No. 05-25, RM-10593, FCC 15-97, ¶ 132 (rel. Aug. 7, 2015) (conditioning approval of ILECs' discontinuance of certain legacy enterprise services on

providers has recently fallen, and many believe that reduced levels of investment will characterize the industry over the future.⁷ This is a step in the wrong direction that threatens to reverse several years of strong, sustained investment in broadband infrastructure. Ongoing infrastructure investment is essential to meeting the nation's broadband deployment goals, and ensuring the success of IoT technologies and services. Regulatory decisions and other government actions that make it harder or less practical to invest, run counter to the Department's goal of encouraging the deployment and adoption of IoT technologies.

As noted in our comments submitted last year to the Broadband Opportunity Council (Council), USTelecom's members have experienced firsthand barriers to broadband infrastructure deployment.⁸ Then, as now, USTelecom encouraged the Department and NTIA to take concrete steps to create and sustain a regulatory environment that provides clear incentives for investment, including the removal of barriers and the promotion of facilities-based competition. The Department and NTIA should work with both Executive branch agencies and independent agencies to remove regulatory barriers to broadband adoption.⁹ By removing such

their commitment to make wholesale services not currently subject to price regulation available at reasonably comparable prices).

⁷ See, Hal Singer, *Does The Tumble In Broadband Investment Spell Doom For The FCC's Open Internet Order?*, Forbes (Aug. 25, 2015) (noting second quarter 2015 declines in capital expenditure by major wireline broadband providers including AT&T, Charter, Cablevision, Verizon, and CenturyLink, ranging from 4 to 29 percent) (available at: <http://www.forbes.com/sites/halsinger/2015/08/25/does-the-tumble-in-broadband-investment-spell-doom-for-the-fccs-open-internet-order/>) (visited June 2, 2016). See also Free State Foundation, *All the Investment We Cannot See* (Sep. 15, 2015) (noting that "infrastructure investment will be *less* going forward than it *otherwise* would be *absent* the FCC's new Internet regulations") (available at: <http://freestatefoundation.blogspot.com/2015/09/all-investment-we-cannot-see.html>) (visited June 2, 2016).

⁸ Comments of USTelecom, *Broadband Opportunity Council Notice and Request for Comment*, Docket No. 1540414365-5365-01 (June 10, 2015).

⁹ For example, in 2014, USTelecom filed with the FCC a petition for forbearance from various

barriers, NTIA can ensure that the robust broadband networks essential to the success of the IoT are deployed throughout the country. NTIA's previous efforts associated with the implementation of the Broadband Technology Opportunities Program (BTOP), should provide the agency with an appreciation for the important role to be played by broadband networks in the IoT space.

III. NTIA Should Urge the Federal Government to Avoid Duplicative and Potentially Overlapping Inquiries and Initiatives in the IoT Space.

The communications and technology industries share a growing concern regarding a constantly expanding and overlapping set of government initiatives related to the emergence of new technologies, services and applications. While government policies can help eliminate impediments to economic growth and innovation, and promote a grounded understanding of public safety and security implications, the lack of coordination across agencies often serves to undermine these objectives. For the Communications Sector, the growing number of initiatives and venues across the government landscape, while important, taxes critical resources and requires the sector to constantly reassess priorities. In its current Notice and Request for Comment, NTIA points to such efforts by the National Highway Traffic Safety Administration (NHTSA) and the Food and Drug Administration (FDA) who "have already begun grappling with potential health, safety and security issues arising from the connection of cars and medical

outdated regulatory requirements applicable only to incumbent local exchange carriers (ILECs). *See*, Petition of USTelecom for Forbearance Pursuant to 47 U.S.C. § 160(c) from Enforcement of Obsolete ILEC Legacy Regulations That Inhibit Deployment of Next-Generation Networks, WC Docket No. 14-192 (filed Oct. 6, 2014). As USTelecom explained in its Forbearance Petition, unlike most broadband providers – including cable, wireless, and competitive fiber providers – ILECs are not free to focus their expenditures on next-generation networks designed to deliver the higher-speed broadband services customers increasingly crave; instead they "must direct a substantial portion of their expenditures to maintaining legacy networks and fulfilling regulatory mandates whose costs far exceed any benefits." *Id.*, at 3. The Department and NTIA should encourage the FCC to remedy this imbalance in regulatory requirements.

devices to the Internet. NTIA also notes that the Federal Trade Commission (FTC) “has identified privacy and cybersecurity aspects of IOT and proposed some possible best practices.”¹⁰

NTIA can play a critical role spanning diverse efforts to ensure that government resources are applied in an efficient and accountable manner, that efforts in individual agencies are consistent with the federal government’s overall policy, and that independent regulatory agencies are discouraged from applying sector-specific rules that could interfere with market forces and delay the benefits to consumers. NTIA is in fact, in a unique position as it can make important recommendations when it produces the “green paper” as described in the Notice.¹¹

As a foundational matter, NTIA should establish a uniform approach for the government in monitoring and addressing evolving IoT issues. USTelecom believes that a silo or vertical approach to IoT applied to a specific industry segment will inevitably produce a Tower of Babel where terminology, standards, best practices, and rules will inevitably conflict and burden every participant in the ecosystem with unnecessary complexity and uncertainty. Valuable resources would be wasted on sorting through a maze of requirements and mandates, adding unnecessary costs and marketing delays. A horizontal approach that builds on commonalities across diverse sectors, infrastructures, devices, services and with an eye towards integration and an enhanced customer experience is far superior. For example, the FTC can handle IoT privacy whether technologies are deployed in agriculture, automobiles, home services, medical devices or any one of many other applications. Instances of vertical regulation should occur only in very unique circumstances and be narrowly tailored to address a critical and unique element of the technology.

¹⁰ *Notice*, p. 19957.

¹¹ *See e.g., Notice*, p. 19956.

Most importantly, NTIA can be a leading voice for promoting economic development by championing IoT, identifying and providing incentives for standards development, identifying the security elements that must be addressed to protect the national infrastructure and championing interoperability across vertical sections of the economy, the networks and service gateways. Through its current policy roles and a key component of the Department of Commerce, NTIA has experience in facilitating highly effective multi-stakeholder processes and can bring together the key Federal departments and agencies that are needed to forge an evolving and sustainable consensus.

IV. NTIA Should Encourage Government to Apply a Voluntary Multi-Stakeholder Collaborative Approach or a Light-Touch Regulatory Approach Only When Necessary.

In recent years, U.S. Government policy in an area of critical impact on IoT, namely cybersecurity, has been predicated on the assumption that a partnership between industry and government is superior to any prescriptive compliance regime, which, by its nature, would lack flexibility to respond promptly to new threats and potentially undermine security by providing the playbook for bad actors to exploit.¹² Following a year-long effort by NTIA's sister agency NIST to develop the Cybersecurity Framework, it is now widely acknowledged that a voluntary and non-prescriptive risk management approach based on a common security taxonomy is more likely to produce sought-after results than reliance on traditional regulatory mandates. IoT will no doubt create a larger attack surface for bad actors interested in disrupting services or exploiting weaknesses for financial or other benefits. For these and other reasons, it is essential that the approach taken by the U.S. Government is thoughtful and based on processes that have

¹² See e.g., Executive Order, *Improving Critical Infrastructure Cybersecurity*, February 12, 2013 (available at: <https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>) (visited June 2, 2016).

been proven to be successful.

USTelecom acknowledges that well-considered and informed regulation is a key part of the evolving ecosystem. NTIA thus should encourage regulators to work with industry to identify potential cybersecurity gaps and distribute responsibilities across the broad ecosystem of device manufactures, applications developers, network service providers and others. Regulators need not follow a traditional notice, comment and rulemaking track but instead can adopt more innovative and flexible means of collaboration with industry. The FCC's Communications Security Reliability and Interoperability Council (CSRIC) serves as an important example of a regulatory agency facilitating effective multi-stakeholder engagement to identify best practices when considering new technologies and security-related threats.¹³ Over a period of many years, CSRIC has been convened to bring leading technologists and thought leaders from industry, government, and academia to collaborate to address a variety of challenges, identify potential solutions, and to make recommendations that are designed to have a meaningful and positive impact for both providers and consumers.

NTIA has demonstrated unique competencies in bringing together diverse sets of stakeholders to address complex issues associated with the rapidly evolving digital economy. Since 2010 when the Commerce Department established the Internet Policy Task Force to conduct reviews on enhancing Internet privacy, improving cybersecurity, protecting intellectual property, and ensuring the global free flow of information, the Task Force and the agency have taken on numerous topics, expanding their role in building multi-stakeholder consensus policies around emerging technologies. Most recently, issues have included privacy and facial

¹³ See, FCC website, Communications Security, Reliability and Interoperability Council (available at: <https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-1>) (visited June 2, 2016).

recognition technologies, smart city infrastructure and policy, unmanned aircraft systems, and vulnerability disclosures, to name a few. Because the Commerce Department can leverage the expertise across six agencies under its domain, including the Economic and Statistics Administration, the International Trade Administration, the National Institute of Standards and Technologies (NIST), the National Telecommunications and Information Administration (NTIA), the Office of the Secretary, and the U.S. Patent and Trademark Office, it is uniquely qualified to bring diverse talent and knowledge across government and industry.

One recent example of how such multi-stakeholder engagement can mitigate or negate the need for prescriptive regulation in this arena is evidenced by NIST's recently released Framework for Cybersecurity-Physical Systems.¹⁴ The report follows an almost two year effort by industry, academia, and government participants who examined how to standardize cyber-physical systems development to ensure trustworthiness of emerging technologies and efforts to build in security and privacy by design. This first stage of this evolving effort, along with the current NTIA inquiry, can serve as a strong foundation for constructing IoT security standards.

V. NTIA Should Encourage Ongoing Industry Collaboration to Promote Voluntary Standards in the IoT Space.

As with any emerging service, the lack of well-defined industry standards can hinder adoption, or worse, create a vacuum that can be filled in counterproductive ways. NTIA has commenced this important and timely inquiry to address a number of critical questions including how best to support standards bodies that are needed to address issues such as interoperability between various service provider networks and/or gateways.

¹⁴ See, Cyber Physical Systems Public Working Group, Framework for Cyber-Physical Systems, Release 1.0, May, 2016 (available at: https://s3.amazonaws.com/nist-sgcps/cpspwg/files/pwgglobal/CPS_PWG_Draft_Framework_for_Cyber_Physical_Systems_Release_1_0Final.pdf) (visited June 2, 2016).

USTelecom also recognizes that there is an international dimension to these questions and we support the development of common world-wide standards and alliances where they are clearly practical and beneficial. In the global environment where IoT will develop quickly, moving to voluntary international standards will help drive volume pricing on component costs. Other major world-wide economies such as China also have significant market presence and can greatly influence and shape standards, policies, and other factors that will affect adoption. NTIA's leadership on this can help ensure that the U.S. maintains a visible presence in the organizations to help establish and drive U.S. objectives.

As the NTIA Notice indicates, well-recognized international bodies such as the Internet Engineering Task Force (IETF), the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), the (ISO/IEC JTC1) and the International Telecommunications Union (ITU) have all initiated work related to IoT. A key area of interest for USTelecom members is in ensuring that any standards that are adopted are voluntary best practices versus prescriptive technical mandates. Additionally, many IoT devices communicate wirelessly, making the availability of spectrum an important factor.

VI. IoT Specific Privacy Regulation is Unnecessary.

In its Notice, NTIA asks how the government should address or respond to privacy concerns about IoT.¹⁵ To answer this question, NTIA should look toward the time-tested approach to privacy utilized by the Federal Trade Commission (FTC), based on its knowledge gained through robust enforcement, rulemakings and experience with guidance that provides a flexible and dynamic approach to protecting consumer privacy and supporting innovation and competition. The White House has endorsed the FTC's approach, in particular recognizing that

¹⁵ *Notice*, p. 19959.

the context within which information is provided and the sensitivity of the information matter.¹⁶ The United States has also urged adoption of the FTC approach internationally.

Of particular note, the FTC is appropriately of the view that any privacy framework should be “technologically neutral.”¹⁷ As previously noted, USTelecom maintains that any privacy framework for IoT will be best addressed through a horizontal, and not vertical, approach. The Department and NTIA could consider convening an industry working group to develop a framework, similar to the NIST Cybersecurity Framework that can be applied consistently across IoT applications regardless of the types of services at issue. Instances of vertical regulation should only occur in very unique circumstances and be narrowly tailored.

In its recent report on the IoT, the FTC noted that the industry was in its “relatively early stages,” and that there is “great potential for innovation in this area.” Based on the current status of the IoT space, the FTC concluded that legislation aimed specifically at the IoT “would be premature.”¹⁸ The FTC instead emphasized the importance of developing self-regulatory programs designed for particular industries that “would be helpful as a means to encourage the adoption of privacy- and security-sensitive practices.”¹⁹

USTelecom notes that the FCC currently has an open proceeding proposing new privacy rules applicable only to broadband Internet access service providers, which run counter to a “technology-neutral” approach. The FCC’s pending rulemaking is reliant upon the agency’s

¹⁶ See, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Economy*, pp. 1 and 14 (White House 2015 Consumer Privacy Bill of Rights).

¹⁷ FTC Staff Report, *Internet of Things, Privacy and Security in a Connected World*, January, 2015, p. 49.

¹⁸ *Id.*, p. 48.

¹⁹ *Id.*, p. 49.

earlier reclassification of broadband as a Title II service, and that determination by the FCC is currently on appeal before the Court of Appeals for the District of Columbia Circuit.

If the courts determine that the FCC has authority over broadband privacy, USTelecom and several other industry associations urged the agency to focus on four privacy principles: (1) transparency; (2) respect for context and consumer choice; (3) data security; and (4) data breach notification. The FCC was encouraged to draw from and harmonize with the longstanding FTC unfairness and deception approach to privacy, which, before the FCC's reclassification decision, governed the privacy practices of all companies in the Internet ecosystem and will continue to apply to non-ISPs going forward.

Prior to the FCC's reclassification of broadband as a Title II service, there was widespread consensus that the privacy framework established by the FTC and applied to all entities in the broadband ecosystem worked effectively to safeguard broadband customer data and foster investment, innovation, and competition. To depart from the FTC's successful framework based upon mischaracterizations of the Internet ecosystem is a mistake and will not only stifle innovation but will also result in consumer confusion. We encourage NTIA to keep this in mind as it considers how to address IoT privacy in this proceeding.

VII. Conclusion

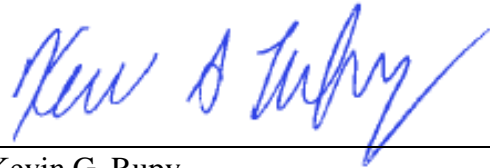
USTelecom appreciates this opportunity to participate in the Department's and NTIA's proceeding on the IoT. Consistent with USTelecom's recommendations, the Department and NTIA are encouraged to develop policy frameworks that incentivize investment in broadband infrastructure and encourage federal government stakeholders to avoid duplicative and potentially overlapping initiatives in the IoT space. Partnerships between industry and government are superior approaches to the IoT than any prescriptive compliance regime, and NTIA should encourage ongoing industry collaboration to promote voluntary standards in the

IoT space. Finally, NTIA should look toward the time-tested approach to privacy utilized by the FTC. That approach – endorsed by the White House – recognizes that the context within which information is provided and the sensitivity of the information matter.

Respectfully submitted,

UNITED STATES TELECOM ASSOCIATION

By:



Kevin G. Rupy
Robert Mayer

Its Attorneys
607 14th Street, NW, Suite 400
Washington, DC 20005
(202) 326-7300

June 2, 2016