Before the
DEPARTMENT OF COMMERCE
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION

In the Matter of	)	
	)	
Green Paper: Fostering the Advancement of the Internet of Things	)	NTIA Request for Comment
	)	Docket Number 17010523-7023-01

COMMENTS OF NTCA–THE RURAL BROADBAND ASSOCIATION

March 13, 2017

TABLE OF CONTENTS

Before the
DEPARTMENT OF COMMERCE
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION

In the Matter of	)	
	)	
Green Paper: Fostering the Advancement of the Internet of Things	)	NTIA Request for Comment Docket Number 17010523-7023-01

COMMENTS
OF
NTCA–THE RURAL BROADBAND ASSOCIATION

I. INTRODUCTION & BACKGROUND

NTCA–The Rural Broadband Association ("NTCA") hereby submits these comments in response to the National Telecommunications and Information Administration ("NTIA") Request for Comments on the "Fostering the Advancement of the Internet of Things" Green Paper.[1] This NTIA Green Paper discusses the analysis of stakeholder comments received in response to the April 2016 IoT Request for Comment on "The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things."[2] The NTIA Green Paper discusses the current policy environment for the Internet of Things ("IoT") and solicits comment on how NTIA can foster continued advancements in that space.

NTCA represents approximately 850 independent, community-based telecommunications companies and cooperatives, and more than 400 other firms that support or are themselves engaged in the provision of communications services in the most rural portions of America in 46 states. All of NTCA's service provider members are full service rural local exchange carriers

---

[1] Request for Comments on the NTIA Green Paper: Fostering the Advancement of the Internet of Things, NTIA Docket No. 17010523–7023–01, 82 Fed. Reg 4313 (rel. Jan. 13, 2017) ("Green Paper").

[2] Request for Comments on the Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things, NTIA Docket Number 160331306-6306-01, 81 Fed. Reg.19956 (rel. Apr. 5, 2016) ("April 2016 IoT Request for Comment").

("RLECs") and broadband providers, and many provide fixed and mobile wireless, video, satellite and other competitive services in rural America as well. NTCA members and small businesses like them provide broadband and other communications services in some of the nation's most difficult to serve rural areas, serving less than *five percent* of the population of the United States across *approximately 37 percent* of the nation's landmass. These companies operate in rural areas long ago left behind by other service providers because the markets were too sparsely populated, too high cost, or just too difficult to serve in terms of terrain. NTCA members have overcome these challenges to deploy advanced communications infrastructure that responds to consumer and business demands, and connects rural America with the rest of the world.[3]

Comments submitted in June 2016 by a diverse group of stakeholders[4] reveal several areas of consensus that should inform consideration of the role of government with respect to IoT issues going forward: (1) any government involvement in this marketplace must focus on voluntary "best practices" that avoid unnecessary or excessive regulatory encumbrances; and (2) a significant amount of infrastructure – both wireline and wireless – will be necessary to ensure that the IoT market flourishes. NTCA discusses below the interdependency of these items – that is, how a "best practices" approach to government involvement in the IoT marketplace can

---

[3] In April of 2016, the Hudson Institute, in conjunction with the Foundation for Rural Service (FRS), released a report examining the economic benefits of rural broadband infrastructure. This report determined that the investments and ongoing operations of small rural broadband providers contribute $24.1 billion annually to the nation's gross domestic product, with 66 percent ($15.9 billion) of that amount accruing to the benefit of urban areas. The report also found that rural broadband investment is an important driver of job growth, estimating that 69,595 jobs – 54 percent of which are with vendors and suppliers in urban areas – can be attributed directly to economic activity of small rural broadband providers. The Hudson Institute, "The Economic Impact of Rural Broadband," April 2016, ("Hudson Paper"), available at: https://s3.amazonaws.com/media.hudson.org/files /publications/20160419 KuttnerThe EconomicImpactofRuralBroadband.pdf.

[4] *See generally*, comments in response to the April 2016 IoT Request for Comment on "The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things" paper, available at: https://ntia.doc.gov/federal-register-notice/2016/comments-potential-roles-government-fosteringadvancement-internet-of-things.

enable and encourage broadband providers to continue investing in the underlying broadband infrastructure necessary for the IoT to flourish.

II. BROADBAND INFRASTRUCTURE IS THE FOUNDATION OF THE IoT.

Broadband providers of all kinds continue to invest heavily in networks in response to consumer demand. Yet, despite the tremendous progress rural broadband providers have made in connecting rural America, the job of deploying and operating the critical broadband infrastructure they have made possible is not finished. Small, rural providers still face the challenges of sustaining and upgrading existing networks to keep pace with consumer demand, delivering affordable services, and extending these networks into parts of rural America still lacking access – particularly as developments in IoT capabilities stimulate even greater consumer demand. Indeed, overcoming these challenges to availability and sustainability of broadband is the condition precedent to the widespread availability of IoT enabled devices that can transform the lives and businesses, especially agricultural operations, for millions of rural Americans. In short, the IoT is not achievable absent robust and ubiquitous *wireline and wireless infrastructure*; broadband infrastructure is, in effect, the foundation upon which the IoT will be built.

As comments in response to the April 2016 IoT Request for Comment[5] stated, and as NTCA recently stated in the Federal Communications Commission's ("FCC's") proceeding on streamlining the deployment of small cell infrastructure,[6] the continued expansion of the IoT

---

[5] *See, e.g.*, Comments of Verizon in NTIA Docket Number 160331306-6306-01 (fil. Jun. 2, 2016), p. 10 (stating that "[a] successful IoT environment will need sufficient radio frequency spectrum and robust communications infrastructure."); Comments of Cisco in NTIA Docket Number 160331306-6306-01 (fil. Jun. 2, 2016), p. 2 ("There is no doubt that the advancement of the IoT will require unprecedented coordination among a myriad of government and industry stakeholders, substantial investments in technology and infrastructure, and a flexible and supportive regulatory and policy environment."); Comments of the National Cable & Telecommunications Association in NTIA Docket Number 160331306-6306-01 (fil. Jun. 2, 2016), p. 4.

[6] Comments of NTCA–The Rural Broadband Association in the FCC WT Docket No. 16-421 (fil. Mar. 8, 2017) (stating that "wireless networks rely heavily on the landline network, and this reliance will only increase with 5G, since only a small portion of the last-mile customer connection (i.e., the local loop) will use wireless technologies").

marketplace will be entirely dependent on robust and ubiquitous wireline and wireless infrastructure. The benefits of the IoT will only be realized by rural and urban Americans alike if the necessary underlying wireline and wireless broadband infrastructure is available, affordable, and capable of handling the increased demands arising out of such data transmission.

Continuing the path of multi-stakeholder, industry-led working groups that include network operators large and small represents one of the most significant steps toward making broadband infrastructure – the foundation of the IoT – available as fast as possible. A "light-touch" regulatory environment that minimizes burdens and barriers to deployment and instead allows rural broadband providers to focus efforts on deploying and sustaining networks is needed to foster the availability of that critical wireline and wireless infrastructure. Indeed, the NTIA Green Paper recognizes the value of "enabling infrastructure availability and access" and "crafting balanced policy and building coalitions" as it relates to fostering the continued expansion of the IoT.[7] NTCA therefore urges the NTIA to look first to multi-stakeholder industry working groups to examine ways to facilitate and sustain infrastructure deployment as a condition precedent to the growth and ongoing viability of the IoT marketplace.

III. THE IoT SPACE IS TOO DYNAMIC FOR TOP-DOWN, PRESCRIPTIVE POLICIES; "BEST PRACTICES" DEVELOPED BY MULTI-STAKEHOLDER GROUPS REPRESENT THE OPTIMAL WAY TO PROMOTE THE AVAILABILITY AND SUSTAINABILITY OF AN EVOLVING IoT.

Moving beyond the foundational importance of infrastructure to the IoT and considering more generally the proper role of government agencies in the IoT space itself, NTCA is pleased the NTIA Green Paper recognizes that "[t]he risk of premature and excessive regulation is notable given the size of the potential economic benefits to U.S. producers and consumers."[8] As

---

[7] Green Paper, p. 3.

[8] *Id.*, p. 11.

the Green Paper goes on to state, the "[g]overnment's relevance is not only as a potential policymaker and regulator, but also as an *enabler* and adopter of IoT technology."[9] The single biggest key to ensuring that government agencies operate as enablers of IoT is the use of a voluntary, "best-practices based" approach to the IoT space that utilizes the views and expertise of multiple stakeholders. In that regard, the Green Paper correctly identifies as one of its next steps fostering "an enabling environment for IoT technology to grow and thrive, allow the private sector to lead, and promote technology-neutral standards and consensus-based multi-stakeholder approaches to policy making at local, tribal, state, federal, and international levels."[10]

This approach represents the right path for several reasons. For one, NTIA need only look to the success of the National Institute of Standards and Technologies ("NIST") "Framework for Improving Critical Infrastructure Cybersecurity" (the "NIST Cybersecurity Framework") as a study in how a government and industry partnership that involves multiple stakeholders (including small ISPs) can successfully utilize "best practices" based principles in a manner superior to top-down prescriptive rules. The NIST Cybersecurity Framework has produced a method by which entities of all sizes can utilize risk-based best practices tailored to their circumstances to comprehensively, holistically, and dynamically address cybersecurity issues. As discussed further below, NTCA urges that this approach be extended to cybersecurity threats in the IoT space.

An industry led, best-practices based approach to the larger IoT space is not only supported by experience, it is also important because – much like in the cybersecurity area – the IoT is so dynamic. The IoT space is currently expanding and evolving far too rapidly for

---

9 *Id.* (emphasis added).

10 *Id.*, p. 56.

prescriptive, top-down regulations that will likely fail to keep pace. In this regard, again, any general government intervention in the IoT marketplace should be modeled on the current policy framework applicable to cybersecurity concerns – an emphasis on "best practices" created by a broad array of industry stakeholders that can keep pace with the changing landscape.

Finally, NTIA should also factor in the important public safety implications of the IoT as it continues down the collaborative, best-practices approach discussed herein and in the Green Paper. In particular, collaboration with local and state public safety officials is critical. As the National Emergency Number Association ("NENA") stated in response to the April 2016 IoT Request for Comment, "the IoT will bring about fundamental changes in how public safety professionals handle emergency responses."[11] As a subset of the general IoT market, emerging public safety devices hold great promise for consumers, 911 agencies, and emergency response personnel. For instance, ubiquitous building, road, and patient sensors, which seamlessly communicate behind-the-scenes with traditional public safety agencies, may improve emergency response scenarios and related outcomes. However, these benefits can only be realized when relevant data is seamlessly exchanged between systems and devices, which further bolsters the need for underlying industry standards. NTIA and NIST are uniquely positioned to facilitate the global development of critical public safety frameworks, which incorporate emerging technologies and devices. Similar to the larger IoT environment, standards for the public safety IoT market should be developed by incorporating input and feedback from a variety of stakeholders, including representatives from local public safety, rural areas, and small ISPs. Indeed, the continued development and universal adoption of NG911 standards and principles will enable IoT-bolstered improvements in technology.

---

[11] Comments of the National Emergency Number Association ("NENA"), in NTIA Docket Number 160331306-6306-01 (fil. Jun. 2, 2016), p. 2.

IV. THE CHALLENGE OF CYBERSECURITY IN THE IoT MARKETPLACE MUST BE MET WITH A MULTI-STAKEHOLDER, INDUSTRY-LED WORKING GROUP THAT INCLUDES SMALL ISPS, TO ENSURE THEIR UNIQUE NEEDS, CONCERNS, AND LIMITATIONS ARE ADDRESSED.

NTCA supports a collaborative framework for IoT security. As noted above and by those commenting on the April 2016 IoT Request for Comment, much like the IoT, cyber threats and vulnerabilities are constantly evolving, and a traditional, rigid "checklist" approach cannot keep pace with the market. Such an approach will quickly become obsolete in the face of new attack vectors and, in the worst-case scenario, provide bad actors with a road map for cyber assault.

IoT threats are unpredictable, diverse, and growing in sophistication and complexity. As such, a prescriptive regulatory approach is ill advised and fated for defeat. To be clear, regulation has an appropriate role in the security and privacy environment. However, the government cannot successfully address evolving IoT security issues by authorizing regulation via one Federal agency, over one narrow portion of the industry, and based upon one brief snapshot in time. In juxtaposition, a multi-stakeholder approach to create and promulgate industry risk-based best practices is best suited to comprehensively and holistically address dynamic IoT cybersecurity issues.

The Broadband Internet Technical Advisory Group ("BITAG") – a non-profit multi-stakeholder organization which counts among its members device manufacturers, software developers, content producers, consumer groups, and ISPs, among others – released a report in November 2016 highlighting the complex IoT security landscape, and the need for cross-sector collaboration to address IoT vulnerabilities.[12] According to the BITAG report, there are a variety of existing vulnerabilities in consumer IoT – problems which may also extend to commercial

---

[12] BITAG, Internet of Things (IoT) Security and Privacy Recommendations, A Broadband Internet Technical Advisory Group Technical Working Group Report, rel. Nov. 2016, available at: https://www.bitag.org/report-internet-of-things-security-privacy-recommendations.php

enterprise or industrial solutions. For instance, many devices have security vulnerabilities when they are shipped or that later develop. As the working group report states, "IoT device security issues are likely to persist because many devices may never receive a software update, either because the manufacturer (or other party in the IoT supply chain, or IoT service provider) may not provide updates or because consumers may not apply the updates that are already available."[13] Many vendors do not have systems or processes in place to deploy updates to thousands of devices and in some cases, a simplistic IoT device may not be *capable* of receiving updates. BITAG acknowledges, however, that some developers do provide automatic software updates; however, "without authentication and encryption, this approach is insufficient because the update mechanism could be compromised or disabled."[14] IoT devices also may leak private user data, both from the cloud (where data is stored) and between IoT devices themselves. As such, credentials should be unique, i.e. each unit or device should have a unique password, and all communications should be encrypted, validating the certificates of the end points involved in an attempt to avoid man-in-the-middle attacks.

The BITAG report details additional security challenges, and recommends a variety of actions for devices makers, among them: IoT devices should ship with reasonably current software; ensure a mechanism for automated, secure software updates; use strong authentication by default; be tested and hardened; and follow security and cryptography best practices.[15] However, in a testament to the shared responsibility, the IoT supply chain also has a role in

---

13 *Id.*, p. iii.

14 *Id.*, p. ii.

15 *Id.*, p. iv-vi.

addressing security and privacy issues, including vulnerability and bug reporting,[16] and presumably a consumer has the ongoing responsibility to update the device software.

Given the variety of security vulnerabilities inherent in the marketplace, IoT security cannot be addressed in a vacuum; rather, it should be developed and subsequently adopted at the ecosystem level with cooperation and collaboration from various participants, including, but not limited to, device manufacturers, cloud service providers, application and software developers, retailers, ISPs, public interest/consumer trade groups, and other associated stakeholders. A multi-stakeholder process is an effective method to convene a variety of stakeholders with their associated relevant government agencies and thereby ensure consistent policies across the county and around the globe. In addition, any multi-stakeholder, industry-led working group should include representation from small businesses, chiefly small ISPs, to ensure their unique needs, concerns, and limitations are addressed within the resultant discussion and best practice development.

NTCA supports NTIA's proposed path forward, chiefly a multi-stakeholder, collaborative process that brings cross-sector partners to the table. For instance, stakeholders should collectively explore best practices regarding security by design; automated processes for regularly updating and patching devices; consumer education; and threats associated with orphaned, end-of-life devices, among other categories. IoT security is a shared responsibility, and it can only be properly addressed by working together.

V. PRIVACY PROTECTIONS IN THE IoT SPACE SHOULD BE MANAGED BY THE FEDERAL TRADE COMMISSION.

The NTIA Green Paper discusses potential privacy concerns with respect to consumers' use of IoT devices and discusses whether and how to address them via either additional

---

[16] *Id.*, p. vi-vii.

regulation or Congressional action to adopt an IoT privacy framework. NTCA urges NTIA to look to the effective and long-standing privacy framework utilized by the Federal Trade Commission ("FTC") and to eschew any IoT-specific privacy regimes.

With respect to the IoT marketplace and associated privacy concerns, the FTC Section 5 privacy framework offers an optimal approach to this dynamic and rapidly changing industry. The FTC is empowered to initiate actions for a company's breach of promise of how it will protect a customer's information, regardless of industry or vertical sector. And, the FTC can act against deceptive or unfair acts or practices. The primary source for FTC authority is Section 5 of the FTC Act, which prohibits "unfair or deceptive or practices in or affecting commerce." "Unfair or deceptive" is a material representation, omission, or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment. "Practice" is an action that (a) causes or is likely to cause substantial injury to the consumer which is not (b) reasonably avoided by the consumer or (c) outweighed by countervailing benefits to the consumer or competition.[17] These may be violated by: retroactive policy changes; deceitful data collection; improper use of data; unfair design; and, unfair information security practices. In the vein of "notice, choice and security," the FTC umbrella can cover obligations of firms to maintain confidentiality; to collect data only in a manner consistent with stated policies; and, to protect that data.[18]

---

[17] *See,* 15 U.S.C. §45(n). This standard is also incorporated in the Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. 111-203, 124 Stat. 1376, *codified at* 12 U.S.C. § 5511 (2011). This three-prong approach was first articulated in the FTC's "Policy Statement on Unfairness," and later incorporated into the FTC Act. *See,* https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness (last viewed May 26, 2016, 12:27).

[18] *See, FTC v. Wyndham Worldwide Corp.,* 799 F.3d 236 (3d Cir. 2015) (failure to use readily available technology such as firewalls; storage of information in plain text; failure to implement adequate policies; failure to remedy known vulnerabilities; failure to use adequate protocols and passwords; failure to restrict access to network; and failure to follow incident response procedures, taken together, constitute unreasonable behavior).

Within the principles of Section 5, industry has utilized a "notice and choice" form of best practices with the FTC as a potent backstop. The Clinton Administration created the Information Infrastructure Task Force, which in 1995 and 1997 recommended self-regulation. Pursuant to this approach, firms determine the standards and self-articulated rules for data collection, use, and disclosure. By way of example, in the late-1900s TRUSTe symbolized voluntary standards, issuing a seal to websites that agreed to abide by certain practices. And, even as the FTC remains a potent backstop to discourage companies from engaging in "unfair or deceptive" practice, the industry pursues practices that are consistent with consumer demands. As noted by Google as it elucidated a backdrop of Federal and state backstops in support of their sufficiency in a similar context, "[p]rivacy policies are now commonly posted on websites, and businesses compete to provider better privacy protections than their peers."[19]

Section 5 is the basis of a robust body of case law, as well. The statute, coupled with numerous interpretations by the courts, provides firms with comprehensive guidance for current and future practice. This framework can meet changing consumer expectations as to their privacy and resulting marketplace demands. Moreover, once again, the IoT marketplace is at once dynamic and nascent. The government and industry can merely speculate about the type of IoT devices that will be developed and embraced by consumers in years to come, and the overall importance of the market in the lives of consumers is likely to expand faster than any statute or regulation produced by an agency rulemaking process. In addition, not every single IoT device uses or has access to customers' data in the same way, or even access to the same data (a smart refrigerator versus a connected heart rate monitor, for example). Thus, a privacy regime based on an evolving body of case law can address violations of consumers' expectations as to their

---

[19] *Expanding Consumers' Video Navigation Choices; Commercial Availability of Navigation Devices: Comments of Google, Inc.*, Docket Nos. 16-42, 97-80, at 7 (internal citation omitted).

privacy when using IoT devices much quicker, yet prevent the industry's expansion from being bogged down by the traditional rulemaking process.

In addition, the use of the FTC Section 5 framework will represent a logical extension of that agency's expertise and broad experience in the privacy field more generally, as well as the FTC's existing work in the IoT privacy arena[20] more specifically. As to the former, the FTC has a significant amount of experience in bringing enforcement actions against hundreds of companies of all sizes and representing a broad section of the communications landscape.[21] With that in mind, it would be shortsighted and counterproductive to fail to leverage that experience. A move away from FTC-based enforcement of privacy norms or an IoT-specific privacy regime would upend settled expectations and practices and confuse or even confound consumer expectations based on little evidence that doing so would be to the benefit of consumers. As to that latter point, there is no indication that the IoT represents a unique privacy threat beyond the use of, for example, Google or Amazon or any of the thousands of business entities already subject to the FTC's jurisdiction, some of which have already been subject to enforcement proceedings. The FTC should, for now, be the default agency to be the "privacy cop on the beat" in the IoT space (as it is in so many others) until such time as it might become clear that consumers' privacy expectations are not being met in a unique way in the IoT space.

---

20 *See, Internet of Things, Privacy and Security in a Connected World*, Staff of the Federal Trade Commission, (rel. Jan. 2015), available at: https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/ 150127 iotrpt.pdf.

21 Comments of the Staff of the Bureau of Consumer Protection, WC Docket No. 16-106 (fil. May 27, 2016), p. 4 (stating in the FCC's 2016 Broadband Privacy proceeding that "[t]o date, the FTC has brought over 500 cases protecting the privacy and security of consumer information."). In their 2016 comments to the FCC, the Federal Trade Commission staff pointed to enforcement actions taken against communications and technology companies of all sizes and for actions such as deceptive uses of customer data and failures to properly secure customer data.

VI. CONCLUSION

For all of the reasons discussed above, NTIA should continue down the path of multi-stakeholder, industry-led working groups that include network operators large and small, as this represents one of the most significant steps toward making broadband infrastructure – the foundation of the IoT – available as fast as possible.

Respectfully submitted,

By: /s/ Michael R. Romano
Michael R. Romano
Senior Vice President –
Industry Affairs & Business Development
mromano@ntca.org

By: /s/ Brian J. Ford
Brian J. Ford
Regulatory Counsel
bford@ntca.org

By: /s/ Jesse Ward
Jesse Ward
Director, Industry & Policy Analysis

4121 Wilson Boulevard, Suite 1000
Arlington, VA 22203
703-351-2000 (Tel)

March 13, 2017