U.S. 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 THE NATIONAL CABLE & TELECOMMUNICATIONS ASSOCIATION

The National Cable & Telecommunications Association ("NCTA")[1] hereby submits its comments on the above-captioned Notice and Request for Public Comment ("Notice").[2]

INTRODUCTION

In this inquiry, NTIA seeks to review "the current technological and policy landscape" surrounding what has come to be known as the "Internet of Things" ("IoT"). The Notice defines that name as an amorphous and

> broad umbrella term that seeks to describe the connection of physical objects, infrastructure, and environments to various identifiers, sensors, networks, and/or computing capability. In practice, it also encompasses the applications and analytic capabilities driven by getting data from, and sending instructions to, newly-digitized devices and components.[3]

The Internet is itself, of course, an amorphous and broad term that encompasses the network of networks that continues to be deployed and used to transmit and retrieve digital information. In the earliest days of its use by consumers, the Internet generally was a means of sending email and accessing textual information via personal computers and "dial-up" services

---

[1] NCTA is the principal trade association for the U.S. cable industry, representing cable operators serving more than 90 percent of the nation's cable television households and more than 200 cable program networks. The cable industry is the nation's largest provider of broadband service after investing over $230 billion since 1996 to build two-way interactive networks with fiber optic technology. Cable companies also provide state-of-the-art competitive voice service to more than 27 million customers.

[2] 81 Fed. Reg. 19956 (April 6, 2016).

[3] Notice at 19957.

such as CompuServe, Prodigy and America Online, which were, in turn, accessed via consumers' telephones. But ever since cable operators and other broadband providers began investing hundreds of billions of dollars to rebuild and continually upgrade the capabilities of their systems to offer two-way high-speed digital communications, the array of Internet-delivered services has been expanding like the Universe after the Big Bang.

While many of those services continue to be accessed by consumers using their Internet "browsers" via their desktop or laptop computers or mobile devices such as tablets and smart phones, there is a rapidly growing array of devices and appliances whose capabilities depend on or are enhanced by being connected to the Internet. At the same time, while cable operators continue to lead the way in providing the access to the Internet on which these devices and appliances depend, there is also a rapidly growing array of providers and technologies enabling such access. For example, in addition to wireline connections to the Internet most frequently provided by cable operators and telephone companies, consumers also purchase wireless Internet access from the same carriers that provide their wireless telephone service.

Moreover, more and more Internet-enabled devices rely on Wi-Fi service – inside and outside the home – to connect to the wireline Internet access services to which consumers and retail establishments subscribe. Consumers use routers to establish Wi-Fi access throughout their homes not only to use their laptops, tablets and smartphones, but also to listen to music on Internet-connected radios, to set their Internet-connected thermostats, to remotely lock, unlock and grant keyless access to their homes via Internet-connected locks and home security devices. Businesses establish Wi-Fi hotspots to enable customers to access the Internet while shopping or sipping coffee in their establishments. And cable operators and other ISPs are increasingly establishing networks of public hotspots that enable their customers to access the Internet – and

to control their Internet-connected devices *inside* their homes when they are *outside* their homes. In addition to consumers monitoring IoT devices themselves, third parties may provide monitoring services, particularly for home security Internet-enabled devices.

Rightly anticipating both the potentially boundless benefits and the substantial challenges presented by this rapid expansion of the IoT, the Notice seeks to identify "possible roles for the federal government in fostering the advancement of IoT technologies in partnership with the private sector."[4] This is a matter of significant interest to the cable industry, whose investment in, and deployment and management of, Internet facilities and technologies have been fueling the rapid growth and transformations of the Internet from the outset. That investment, deployment and effective management have, in turn, been accompanied and nurtured by a national policy of regulatory restraint – a policy specifically codified in 1996, when Congress directed that "[i]t is the policy of the United States . . . to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, *unfettered by Federal or State regulation.*"[5]

The hallmark of such a policy of regulatory restraint is caution. It consists of closely monitoring marketplace developments but refraining from intervening with regulation so long as the marketplace continues to operate efficiently and to stimulate growth and innovation. And everything about the nascent IoT warrants such an approach. So much about the IoT is uncertain, yet the IoT marketplace appears to be flourishing and constantly expanding the array of competitive choices of new products and services for consumers. What we *do* know is that the continuing growth of the IoT will be accompanied by a need for spectrum – and government can play a necessary role in ensuring that sufficient spectrum is available. In addition, multi-

[4] *Id.* at 19956.

[5] 47 U.S.C § 230(b)(2).

stakeholder work may be helpful in developing voluntary guidelines for the unique security challenges presented by the IoT. With respect to other policy implications and potential governmental action, while the Notice tees up many matters that bear close monitoring, it is far too soon to contemplate regulatory intervention.

I. IT IS NOT TOO SOON FOR GOVERNMENT TO ENSURE THAT THERE IS SUFFICIENT USABLE SPECTRUM FOR THE INTERNET OF THINGS.

While it is difficult at this point to predict with certainty how the IoT will develop, there are some things that we already know with a reasonable degree of certainty. What we know is that the Internet is providing the foundation for an ever-expanding array of devices and services. And we know that as that array grows and grows, the infrastructure on which Internet traffic associated with the IoT relies will need to be sufficiently robust to support that traffic. We also know that a significant portion of that traffic will consist of wireless transmissions connected to the substantial wired infrastructure and servers that make up the "cloud."

Keeping up with the ever-growing use of the Internet to date has already required enormous investment in this infrastructure. For the most part, this is simply a matter of private investment by the companies responsible for building, maintaining and providing the infrastructure. But the *unlicensed spectrum* portion of the infrastructure – the part that makes Wi-Fi possible, and that, in turn, helps enable the use of the Internet on computers, mobile devices, and other "things" not physically connected to the ISP's facilities – needs something else that cannot be provided without the government's assistance. That something is *spectrum* – in this case, the unlicensed spectrum that is at the heart of Wi-Fi and will be at the heart of the IoT.

Government needs to ensure that sufficient unlicensed spectrum is available for these purposes. In 2014, the Federal Communications Commission (FCC) took an important step in

this direction by making available additional unlicensed spectrum for high-speed, high-capacity Wi-Fi and other unlicensed uses in the 5 GHz band.[6] As the record in the FCC's proceeding showed, such a step was necessary to ensure enough spectrum simply for the projected growth of Wi-Fi for traditional Internet access by mobile phones and tablets.[7] But as the Notice in this proceeding recognizes, as the IoT develops, "the number of connected devices is expected to grow exponentially."[8] This means that the FCC will need to continue to monitor spectrum needs and usage and to make sufficient licensed and unlicensed spectrum available for Wi-Fi and the IoT ahead of demand.

In addition, NTIA has an important role to play in ensuring that sufficient unlicensed spectrum is made available to support the IoT. In January 2013, NTIA released a study examining the feasibility of sharing up to 195 megahertz of spectrum in the 5 GHz band by federal entities and privately-operated unlicensed devices.[9] NTIA noted that its report was an initial study, and stated that it would conduct additional quantitative analyses "which will include additional analysis and measurements to evaluate the feasibility of existing, modified, proposed and new spectrum-sharing technologies and approaches."[10] NTIA should expeditiously proceed with these efforts to find workable solutions to spectrum sharing in the 5 GHz band, which will lead to the availability of additional unlicensed spectrum for the IoT.

---

6 *In the Matter of Revision of Part 15 of the Commission's Rules to Permit Unlicensed National Information Infrastructure (U-NII) Devices in the 5 GHz Band*, First Report and Order, 29 FCC Rcd 4127 (2014).

7 *See, e.g., id.* at 4156.

8 Notice at 19957.

9 *Evaluation of the 5350-5470 MHz and 5850-5925 MHz Bands Pursuant to Section 6406(b) of the Middle Class Tax Relief and Job Creation Act of 2012*, U.S. Department of Commerce, https://www.ntia.doc.gov/files/ntia/publications/ntia_5_ghz_report_01-25-2013.pdf (Jan. 2013).

10 *Id.* at ii.

In addition to increasing spectrum availability, it will be necessary to establish rules of the road that prevent other users that share spectrum with Wi-Fi from unduly interfering with Wi-Fi and IoT usage. For example, NCTA has already alerted the FCC that the use by licensed wireless carriers of a new technology called LTE-U could cause massive interference problems for Wi-Fi users of the 5 GHz spectrum.[11] Unlike Wi-Fi, LTE-U has not participated in the development of industry standards to ensure fair and collaborative sharing and co-existence of unlicensed users. The expanded availability of unlicensed spectrum will not serve its purpose of facilitating the IoT if LTE-U devices make the spectrum less usable for Wi-Fi and the IoT devices that rely on it.

II. IT IS FAR TOO EARLY IN THE DEVELOPMENT OF THE INTERNET OF THINGS TO CONTEMPLATE GOVERNMENT INTERVENTION.

Beyond the obvious need for sufficient spectrum, we know far too little about how the nascent IoT will develop to warrant regulatory actions by the Government. The IoT is likely to be comprised of an array of disparate and discrete services and devices – from online medicine to online kitchen appliances – that have little more in common than their use of the Internet. One-size-fits-all regulation of all these devices is unlikely ever to be warranted, and it is too soon to attempt even to answer with any confidence the broad economic, technological and policy questions raised in the Notice, much less to overlay the IoT with broad, top-level regulations regarding those issues.

This is not to say that the concerns underlying those questions are not being addressed by the IoT stakeholders while the marketplace evolves. Participants in this growing portion of the economy have an interest in ensuring the compatibility, security, and usability of connected

[11] *See* NCTA Comments, In the Matter of Office of Engineering and Technology and Wireless Telecommunications Bureau Seek Information on Current Trends in LTE-U and LAA Technology, ET Docket No.15-10 (June 11, 2015), https://www.ncta.com/sites/prod/files/2015-06-11_NCTALTEU-PN-Comments.pdf.

devices and the IoT. Several organizations (including the cable industry's research and development consortium, CableLabs) are serving as collaborative laboratories to address these issues in order to ensure that the benefits of the IoT are made available as swiftly as possible.

In particular, issues of cybersecurity are at the forefront of ongoing multifaceted efforts by Internet technologists and stakeholders, including cable operators and other ISPs. The exponential growth in the number and types of devices connecting to the Internet presents a unique challenge to ensuring the cybersecurity of broadband networks and their customers. Unlike traditional connected devices such as computers and smart phones, connected appliances, cameras, and other consumer equipment with new abilities to connect to the Internet may lack the user interfaces, internal capabilities, and external monitoring to enable consumers, equipment manufacturers and others to update security software or defend against attacks. Moreover, these new types of connected devices may stay connected to the Internet far longer than the average computer or smart phone, potentially extending the threat to security of the Internet from obsolete software.

What IoT devices need, initially, is continuing attention from their designers and/or from the services with which the devices are used. Cybersecurity depends upon continuing software updates to Internet-connected computers and devices, including IoT devices, in order to keep up with and thwart hacks and attacks. And, as the universe of such devices expands, the threat posed by orphan devices – devices no longer supported by their manufacturers – will need to be addressed. Some way will have to be found to ensure that devices that consumers continue to use to connect to the Internet can be updated and protected, and that, if device manufacturers discontinue devices, there is some mechanism (*e.g.*, transferring the needed software keys to a designated consortium) for ensuring that devices do not function without the software updates

needed to ensure security. Fortunately, stakeholders have a strong interest in the development of cybersecurity standards, and a multi-stakeholder process to establish voluntary guidelines may need to play some role in facilitating solutions to these challenges.

Similarly, on matters of privacy, a multi-stakeholder process is the best way, at this early stage of the IoT, to develop a consistent data privacy framework for the entire Internet ecosystem that both protects consumers and preserves industry flexibility to innovate. On these matters, and, indeed, on *all* matters related to the IoT – the cable industry has a strong interest in ensuring that their customers continue to enjoy the fullest benefits of the Internet. Marketplace forces, infused with existing competition throughout the Internet ecosystem, are most likely to produce this outcome, and, in any event, as the Federal Trade Commission's Staff Report on the IoT concluded last year, it is too soon even to contemplate extending new regulation any further into this developing marketplace:

> The Commission staff recognizes that this industry is in its relatively early stages. Staff does not believe that the privacy and security risks, though real, need to be addressed through IoT-specific legislation at this time. Staff agrees with those commenters who stated that there is great potential for innovation in this area, and that legislation aimed specifically at the IoT at this stage would be premature. Staff also agrees that development of self-regulatory programs designed for particular industries would be helpful as a means to encourage the adoption of privacy- and security-sensitive practices.[12]

[12] FTC Staff Report, *Internet of Things: Privacy and Security in a Connected World* (January 2015).

Nevertheless, NCTA welcomes NTIA's efforts to identify and highlight the many issues surrounding the successful development of the IoT and the role of the government in monitoring, fostering – and staying out of the way of – this outcome. And we look forward to commenting on the "green paper" that may result from this initial inquiry.

Respectfully submitted,

/s/ Rick Chessen

Rick Chessen
Michael S. Schooler
National Cable & Telecommunications Association
25 Massachusetts Avenue, N.W. – Suite 100
Washington, D.C. 20001-1431
(202) 222- 2445

June 2, 2016