Before the
National Telecommunications and Information Administration
Department of Commerce
Washington, DC

In re	
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
COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION

Pursuant to the Request for Comment[1] (RFC) issued by the National Telecommunications and Information Administration (NTIA) and published in the Federal Register at 81 Fed. Reg. 19,956 (April 6, 2016), the Computer & Communications Industry Association (CCIA) submits the following comments on the subject of fostering the advancement of the Internet of Things (IoT).

I. Introduction

CCIA represents large, medium, and small companies in the high technology products and services sectors, including computer hardware and software, electronic commerce, telecommunications, and Internet products and services. Our members employ more than 750,000 workers and generate annual revenues in excess of $540 billion.[2]

CCIA commends NTIA for its framing in this Request for Comment, and the balanced discussion of the benefits of and potential challenges facing the Internet of Things. In defining the government's potential role in the forthcoming Green Paper, it is crucial to maintain this

[1] Notice, Request for public comments, *The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things,* 81 Fed. Reg. 19956 (April 6, 2016), *available at* https://www.federalregister.gov/articles/2016/05/11/2016-11124/the-benefits-challenges-and-potential-roles-for-the-government-in-fostering-the-advancement-of-the [hereinafter "NTIA Request for Comment"].

[2] A list of CCIA members is available at http://www.ccianet.org/members.

balance to ensure that the full benefits of the IoT are realized for the consumer, industry, and government alike.

II. What is the Internet of Things?

Importantly, at the outset of its RFC, NTIA seeks to understand what sorts of devices, services, and infrastructure comprise the "Internet of Things."[3] The RFC describes IoT as a "broad umbrella term that seeks to describe the connection of physical objects, infrastructure, and environment to various identifiers, sensors, networks, and/or computing capability."[4] NTIA further notes, "In practice, it also encompasses the applications and analytic capabilities driven by getting data from, and sending instructions to, newly digitized devices and components."[5]

The Request for Comment's description of IoT is useful is demonstrating the wide variety of devices, markets, and use cases that might develop. IoT devices and associated services can range from simple and low-cost, like a smart light bulb, to complex and analytically powerful, like personal health monitoring devices or smart electric grid technologies.

However, this sort of description, while expansive, can also lead to confusion because it does not reflect what the Internet of Things looks like from the perspective of consumers. When consumers purchase a "connected device," they are getting both a good and a service—the physical device's connection often comes paired with a service operated remotely, often without a separate monthly service fee. True, the consumer may also see an application interface used to control or view data from a connected device, but that app is just an aspect of the services associated with that particular purchased "thing." It is important to ensure that the inherent duality found in IoT products is reflected in the context of any consumer protective best practices going forward.

III. The Internet of Things will lead to significant economic benefits and innovation.

The Internet of Things, in all its iterations of connected devices, sensors, and services, will account for an increasing share of networked connections worldwide. Gartner forecasts that

[3] NTIA Request for Comment at 19957.
[4] *Id.*
[5] *Id.*

6.4 billion connected "things" will be in use in 2016—30 percent more than in 2015, but dwarfed by the 20.8 billion estimated for 2020.[6]

As these billions of connections come online, IoT devices and sensors will by design, collect, collate, disseminate, analyze, and act on data, producing insights that could transform numerous industries. Data from IoT devices will be used to identify markets and business opportunities, optimize services in a host of industries, and produce the meaningful insights necessary to develop new products and services that will bring currently offline sectors into the digital ecosystem. The most commonly cited examples of these newly connected industries include cars,[7] home appliances,[8] and healthcare,[9] while the ability to glean data from widely deployed sensors will also improve processes across supply chains, increase efficiency in the energy sector,[10] and lead to better functioning cities.[11]

The economic benefits that will likely inure from the Internet of Things could range from $4 trillion to $11 trillion in the ten years from 2015 and 2025.[12] To ensure that those substantial economic benefits are realized, there are a range of pro-innovation policies that governments should promote to foster innovation and growth in and through IoT.

IV. Policy, law, and regulation should be designed to foster the development and adoption of the Internet of Things.

The Internet of Things, for all its promise, naturally raises some concerns of potential risks to consumers as previously offline sectors connect to the wider Internet. The increasing numbers of connected devices and greater quantity of associated data should not necessarily

[6] Press Release, Gartner, Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015, (Nov. 10, 2015) http://www.gartner.com/newsroom/id/3165317.

[7] *See Smartphones on wheels*, ECONOMIST.COM (Sept. 6, 2014), http://www.economist.com/news/technology-quarterly/21615060-way-cars-are-made-bought-and-driven-changing-mobile-communications.

[8] *See* Chris Morris, *Ordinary Home Appliances Are About to Get Really Sexy*, FORTUNE.COM (Jan. 6, 2016, 2:08 PM), http://fortune.com/2016/01/06/home-appliances-ces-2016/.

[9] *See* Nile Lars, *Connected Medical Devices, Apps: Are They Leading the IoT Revolution – Or Vice Versa?*, WIRED.COM, http://www.wired.com/insights/2014/06/connected-medical-devices-apps-leading-iot-revolution-vice-versa/ (last visited June 1, 2016).

[10] *See* Office of Electricity Delivery & Energy Reliability, Technology & Development: Smart Grid, ENERGY.GOV, http://energy.gov/oe/services/technology-development/smart-grid (last visited June 1, 2016).

[11] *See* Release from the Office of the Press Secretary, FACT SHEET: Administration Announces New "Smart Cities" Initiative to Help Communities Tackle Local Challenges and Improve City Services,WHITEHOUSE.GOV (Sep. 14, 2015), https://www.whitehouse.gov/the-press-office/2015/09/14/fact-sheet-administration-announces-new-smart-cities-initiative-help.

[12] James Manyika et al., *Unlocking the potential of the Internet of Things*, MCKINSEY GLOBAL INSTITUTE (June 2015), http://www.mckinsey.com/business-functions/business-technology/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world.

entail the creation of new laws and regulatory regimes specific to IoT. As with any nascent technology, legislators and regulators should take a light-touch approach with the Internet of Things. As the Federal Trade Commission (FTC) determined in its recent examination of IoT, "there is great potential for innovation in this area, and . . . IoT-specific legislation would be premature"[13]— instead, there should be evidence of real, IoT-specific harms to consumers before new rules are considered.

However, the Internet of Things is not emerging in a regulatory vacuum. The data and activities associated with the most sensitive applications of connected devices and services are already subject to the protections of existing rules and oversight, covering areas including privacy, data security, energy, finance, and transportation. Ensuring that these existing regimes are applied, when appropriate, to IoT in a manner that promotes innovation, is key.

If any new rules are determined to be necessary, they should be voluntary and principle-based. As discussed earlier, the Internet of Things includes an extraordinary range of devices, services, and use cases. No single regulatory or legal regime or set of standards intended to apply to such a diverse array of systems and uses will successfully protect consumers and allow IoT to realize its fullest potential. Where appropriate, the government, and NTIA in particular, should employ its power to convene to encourage the development of industry-wide best practices and self-regulatory regimes for the Internet of Things, as these tools have proven effective in other contexts, including traditional media and digital advertising.

A. Privacy and data protection

Consumer privacy is one area where existing regulation and enforcement effectively protect the data collected and used by IoT devices and services, even in the most sensitive of circumstances. An existing array of sector-specific privacy laws exist that protect children,[14] financial data,[15] health information,[16] and data used when making credit, insurance, employment, and housing decisions.[17] The requirements of these laws would remain applicable to producers and operators of connected devices and services.

[13] FTC STAFF REPORT, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD 49 (Jan. 2015), *available at* https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf [hereinafter "FTC IoT Report"].

[14] Children's Online Protection Privacy Act, 15 U.S.C. § 6501-6506 (1998)

[15] Gramm-Leach-Bliley Act, 15 U.S.C. § 6801-6809 (1999).

[16] Health Insurance Portability and Accountability Act, 42 U.S.C § 1320d et seq. (1996).

[17] Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq. (1970).

Those laws are supported and expanded upon by the authority of the FTC and state Attorneys General. The FTC has broad enforcement authority under section 5 of the FTC Act, which prohibits "unfair or deceptive practice in or affecting commerce."[18] It uses that authority judiciously to enforce privacy promises that all companies make to consumers and to ensure that they employ reasonable best practices in privacy and data security.[19] Complementing the FTC's robust consumer protection powers are the corresponding unfair and deceptive practices authorities enforced by state Attorneys General,[20] and state laws, such as the California Online Privacy Protection Act[21] and the Delaware Online Privacy and Protection Act.[22]

In its recent report on the Internet of Things, the FTC has made clear that it intends to apply its existing privacy regulatory regime to IoT.[23] Absent evidence of real consumer harms, as the FTC noted, it is currently premature to seek legislation to constrict the development of the Internet of Things. Rather, policymakers should be cognizant of the full scope of benefits of IoT when assessing existing privacy regulations. Cost-benefit assessments should take into account that consumer data not only drives innovation in consumer-facing devices, but also fuels non-consumer facing innovation and attendant benefits. For example, smart thermostats allow for better energy grid management and reduced energy use, which provides environmental benefits.

Instead of seeking new legislation, the FTC encouraged consumer advocates and industry to work together to develop voluntary industry best practices for IoT privacy.[24] Consumer trust is critical to the success of the Internet of Things—consumers will not purchase and use connected devices and services if they feel their personal information or private lives would be at risk. Companies have a clear incentive to engage in best practices to ensure that consumer privacy harms are avoided and that data is protected.

---

[18] 15 U.S.C. § 45 (2006).

[19] *See Enforcing Privacy Promises*, FED. TRADE COMM'N, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises (last visited May 26, 2016).

[20] *See* Danielle K. Citron, *Privacy Enforcement Pioneers: The Role of State Attorneys General in the Development of Privacy Law*, NOTRE DAME L. REV., (forthcoming 2016), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2733297.

[21] CAL. BUS. & PROF. CODE §§ 22575-79 (2014).

[22] DEL. CODE tit. 6, § 1201C (2016).

[23] FTC IoT Report at 53.

[24] *See id.* at 49.

B. Cross-border data flows and international engagement

To ensure that the Internet of Things can flourish worldwide, CCIA encourages the Department of Commerce to raise the issues of cross-border data flows and competition in telecommunications networks in ongoing trade negotiations. Currently, international trade rules are not sufficient for supporting competition in telecommunications networks. Free and open flow of data is vital for trade in all sectors; in particular, cross-border barriers in communications could obstruct the development of IoT.

Given the United States' role in the global economy, and the importance of telecommunications networks to trade, the Department of Commerce should advocate strongly for competition and the free flow of data. In particular, the Trade in Services Agreement (TiSA) could help remove these barriers by implementing technology-neutral provisions for the application of broadband wholesale access rules, strengthening transparency and regulatory review requirements, eliminating foreign equity caps, and advocating that TiSA telecom rules be GATS+ and go beyond the provisions found in the Trans-Pacific Partnership.

Flexibility and compatibility in data protection laws are also necessary to promote the cross-border data flows essential to the continued growth of IoT. Data localization requirements, direct and indirect, should be discouraged, as they will hamper the efficiency gains promised by IoT. Constructive examples of the sorts of interoperable data protection regimes that should be promoted by the Department in its international engagements include the APEC Cross-Border Privacy Rules system and the pending EU-U.S. Privacy Shield.

V. Technical standards for the Internet of Things should be flexible, protect consumers, and promote competition.

A. Interoperability and copyright

The Internet of Things (IoT), like the Internet itself, depends upon interoperability: the ability of hardware and software components developed by different companies to communicate with one another. A 2015 McKinsey report concluded that "interoperability is necessary to create 40 percent of the potential value that can be generated by the Internet of Things. . . . Interoperability is required to unlock more than $4 trillion per year in potential economic impact from IoT use in 2025. . . ."[25] These IoT interoperability standards have and should continue to be

[25] McKinsey & Company Report, *The Internet of Things: Mapping the Value Beyond the Hype*, MCKINSEY GLOBAL INSTITUTE 2, 4 (June 2015) *available at*

determined by companies and markets.

Today, a host of standards have been developed to support innovative IoT functionality, and to the extent these standards are not open, reverse engineering may be necessary to ensure consumers can fully benefit from the devices they purchase. Technology developers inevitably will need to overcome various challenges in integrating connected devices, but government mandates and copyright law should not be one of them.

The good news is that a global consensus across courts and policymakers had emerged in stating that copyright does not protect software program elements necessary for interoperability. Unfortunately, a recent decision of the U.S. Court of Appeals for the Federal Circuit in *Oracle Am., Inc. v. Google, Inc.*[26] threatens this consensus. Notwithstanding overwhelming precedent[27] to the contrary, the Federal Circuit stated that program elements necessary for interoperability could receive copyright protection, and the Solicitor General unwisely supported this conclusion.[28] In the Green Paper, NTIA should acknowledge the potential adverse impact that copyright protection for interface rules can have on the development of the Internet of Things. If other courts follow the misguided *Oracle* decision, the open, innovative, and competitive nature of the Internet of Things may be compromised. Indeed, *Oracle* upset previously settled expectations about software interoperability, and has already influenced new, ongoing litigation.[29]

A software application can function only in conjunction with hardware and other software, including an operating system, and can run only on an operating system with which it is "compatible"[30]—that is, one which conforms to the same set of technical rules, known as

---

http://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Business%20Technology/Our%20Insights/The%20Internet%20of%20Things%20The%20value%20of%20digitizing%20the%20physical%20world/Unlocking_the_potential_of_the_Internet_of_Things_Full_report.ashx.

[26] 750 F.3d 1339 (Fed. Cir. 2014).

[27] *See e.g. infra* n.34.

[28] After the Supreme Court declined to grant certiorari, the case was sent back to the district court. Last week a jury found that Google's use of the Java programming language in its Android phones was fair use. This does not change the Federal Circuit's troubling ruling that APIs are copyrightable, but the legal process is still ongoing. *See* Jonathan Band, *Sanity Prevails Again: The Jury Verdict in Oracle v. Google*, DISRUPTIVE COMPETITION PROJECT (May 26, 2016), http://www.project-disco.org/intellectual-property/052616-sanity-prevails-again-the-jury-verdict-in-oracle-v-google/. While the fair use verdict is a positive outcome, small companies will face uncertainty and heavy costs if litigation is required to permit interoperability.

[29] *See, e.g.*, Stephanie Condon, *Oracle vs. Google, Round 2: Trial begins over Java API copyright claim*, ZDNET.COM (May 9, 2016, 5:00 AM), http://www.zdnet.com/article/oracle-vs-google-round-2-trial-begins-over-java-api-copyright-claim/ (discussing the potential impact the case has had on software development, and how *Cisco v. Arista*, filed after the CAFC decision in *Oracle*, includes a claim of infringement resembling Oracle's).

[30] In these comments, the term "compatibility" is used interchangeably with "interoperability."

"interface specifications." In the IoT context, software in devices such as sensors, mobile devices, appliances, and automobiles must conform to similar interface specifications as the other devices with which they communicate. If a company could exercise proprietary control over the interface specifications implemented by its products, that company could determine which products made by other firms—if any—would be compatible with its software. Such a broad monopoly would have serious implications for consumers. In the absence of competition during the effective lifespan of a product, the first developer would have little incentive to develop more innovative and less costly products.[31] If copyright may be used to exclude competitors from accessing *de facto* standard interface specifications, consumers risk being locked into a particular operating system or network software environment, and would inhibit the transfer of data between users with different computing environments.[32]

In short, overly broad intellectual property rules can restrict competition and innovation. In fact, lock-in and high switching costs were the status quo in the computing environment into the 1980s.[33] More recently, however, courts began to find that interface specifications fall on the unprotected side of copyright's idea/expression dichotomy. These more recent rulings enabled the transition from the 1970's locked-in computer environments to today's interoperable Internet. In fact, courts,[34] Congress,[35] U.S. trading partners,[36] and jurisdictions worldwide, from Europe[37]

---

[31] A prominent copyright treatise explains that "late-arriving hardware or software producers must, to compete, make their products compatible with the products sold by entrenched industry leaders, an effort that will characteristically require them to copy the industry leaders' interface specifications – the key that opens the lock to their operating systems." 2 GOLDSTEIN ON COPYRIGHT § 8.5.1 (2d ed. 2005).

[32] *See Lotus Dev. Corp. v. Borland Int'l, Inc.*, 49 F.3d 807, 821 (1st Cir. 1995) (Boudin, J., concurring), *aff'd by an equally divided court*, 516 U.S. 233 (1996).

[33] *See* JONATHAN BAND & MASANOBU KATOH, INTERFACES ON TRIAL 2.0, *infra* n.39, at 1 (2011); *Apple v. Franklin*, 714 F.2d 1240, 1253 (3d Cir. 1983) (stating that compatibility is "a commercial and competitive objective which does not enter into the somewhat metaphysical issue of whether particular ideas and expression have merged"); *see also Whelan v. Jaslow*, 797 F.2d 1222 (3d Cir. 1986) (suggesting that copyright protected all program elements other than the idea of operating a dental laboratory).

[34] *See, e.g.*, *Atari Games Corp. v. Nintendo of America*, 975 F.2d 832 (Fed. Cir. 1992); *Sega Enters. v. Accolade, Inc.*, 977 F.2d 1510 (9th Cir. 1992) (citing 17 U.S.C. § 107). *See also DSC Comms. Corp. v. DGI Techs*., 898 F. Supp. 1183 (N.D. Tex. 1995), *aff'd*, 81 F.3d 597 (5th Cir. 1996); *Bateman v. Mnemonics, Inc*., 79 F.3d 1532 (11th Cir. 1996); *DSC Comms. Corp. v. Pulse Comms. Inc*., 976 F. Supp. 359 (E.D. Va. 1997), *aff'd in part, rev'd in part, and vacated in part*, 170 F.3d 1354 (Fed. Cir. 1999); *Sony Computer Entm't v. Connectix Corp*., 203 F.3d 596 (9th Cir. 2000). Other courts have prevented enforcement under a copyright misuse theory. *See, e.g.*, *Alcatel U.S.A. v. DGI Techs*., 166 F.3d 772 (5th Cir. 1999).

[35] Principles of software compatibility found support in Congress, when it adopted an exception explicitly directed at software reverse engineering and interoperability in 17 U.S.C. § 1201(f). Section 1201(f)(4) defines interoperability "as the ability of computer programs to exchange information, and of such programs mutually to use the information which has been exchanged."

[36] Since 2002, U.S. free trade agreements ("FTAs") have included provisions modeled on the interoperability exception to Section 1201 of the DMCA. *See, e.g.*, U.S.-Korea Free Trade Agreement, art. 18.4.7(d)(i), June 30,

to Asia,[38] had arrived at a consensus interpretation of the copyright question of compatibility over the past 25 years—a consensus disrupted only by the Federal Circuit's recent *Oracle* decision.[39] This decision, and the Solicitor General's support for it, conflicts with the majority of U.S. federal appellate courts, eleven U.S. free trade agreements, and copyright law across the globe. NTIA should take this opportunity to distance the Administration from a minority position on which federal courts are split and which contradicts established principles of international law. In the context of the Internet of Things, NTIA should construe the *Oracle* case as an outlier, confined to its facts, which should not guide policy going forward. In general, and with respect to the IoT specifically, the U.S. Government should adhere to the internationally accepted principle that interface specifications are not regulated by copyright.

B. Patents

As the Internet of Things matures, the risk from patent trolling will increase. Patent assertion entities ("PAEs") have the potential to stifle or severely hinder the development of the IoT. PAEs were responsible for more than sixty percent of patent litigations in 2015,[40] and sixty

---

2007, 8 U.S.T. 2217 (parties may permit "[n]oninfringing reverse engineering activities with regard to a lawfully obtained copy of a computer program . . . for the sole purpose of achieving interoperability of an independently created computer program with other programs."). Interoperability exceptions appear in FTAs with Australia, Bahrain, Chile, Colombia, Costa Rica, Dominican Republic, El Salvador, Guatemala, Honduras, Korea, Morocco, Nicaragua, Oman, Panama, Peru, and Singapore.

[37] In 1991, the European Union adopted a Software Directive, which reflects a policy judgment that copyright should not interfere with interoperability. Council of Ministers Directive 91/250/EEC of 14 May 1991 on the Legal Protection of Computer Programs, 1991 O.J. (L 122). Article 6 of the Software Directive permits reverse engineering "indispensible to obtain the information necessary to achieve . . . interoperability." The legislative process leading to the adoption of the Directive is discussed in detail in INTERFACES ON TRIAL, *infra* n.39, at 227-41. The Software Directive has been implemented by all member states of the EU, as well as Norway, Russia, Switzerland, and Turkey. INTERFACES ON TRIAL 2.0, *infra* n.39, at 6. Commentators generally perceived that "the law on software copyright interoperability issues seem[ed] quite settled on both sides of the Atlantic." Pamela Samuelson, *The Past, Present, and Future of Software Copyright Interoperability Rules in the European Union and United States*, 34(3) EUR. INTELL. PROP. REV. 229 (2010). In 2012, Europe's highest court, the CJEU, reached precisely the same conclusion as the district court in *Oracle*, and the opposite of the Federal Circuit, in *SAS Institute, Inc v. World Programming Ltd* [2012] 3 CMLR 4, ¶ 40 (holding that the Software Directive "must be interpreted as meaning that neither the functionality of a computer program nor the programming language and the format of data files used in a computer program in order to exploit its functions constitute a form of expression of that program and, as such, are not protected by copyright. . .").

[38] *See* INTERFACES ON TRIAL 2.0, *infra* n.39, at 136-67, 175.

[39] This history is discussed in detail in Jonathan Band & Masanobu Katoh, Interfaces on Trial: Intellectual Property and Interoperability in the Global Software Industry (1995), *available at* http://www.policybandwidth.com/interfaces-2-0; *see also* Band & Katoh, Interfaces on Trial 2.0 (2011), *available at* http://mitpress.mit.edu/books/interfaces-trial-20.

[40] RPX, *2015 Report: NPE Litigation, Patent Marketplace, and NPE Cost* 7 (2016), *available at* https://www.rpxcorp.com/wp-content/uploads/sites/2/2016/05/RPX-2015-Report-NPE-Litigation_Patent-Marketplace_Cost_High-level_ZFinal.pdf.

percent of the defendants were small businesses (i.e., businesses with less than $100 million in annual revenue).[41] Sixty-seven percent of the patents used by PAEs were in technology areas related to the Internet of Things.[42]

As a result, businesses providing IoT products and services will be potential targets for PAEs, particularly once they have the cash available to pay settlements.[43] This additional risk may deter businesses from investing in the IoT and will, at a minimum, reduce the available capital for investment in IoT products and services.

C. Securing the Internet of Things

The number of "things" comprising the Internet of Things is growing at a prodigious rate. As mentioned, Gartner estimates that there will be 20.8 billion connected devices in use by 2020, while Cisco believes there will by 37 billion such devices worldwide, generating at least 507.5 zettabytes of data per year.[44] As traditionally offline sectors become connected, ensuring that the vast volume of data they collect, produce, and use is secure will be imperative, especially because many of those sectors, namely home appliances, transportation, healthcare, and finance, will be awash with particularly sensitive data and enable novel autonomous activities.[45]

To maintain consumer trust in IoT devices and services, companies must protect and secure the data they collect and use in all contexts. Encryption is a fundamental aspect of this data security regime, and should play a role in all aspects of the IoT ecosystem, including at the device level, for data in transit, and at the platform or service level. Governments should not mandate particular technical standards for the type of encryption deployed, as that will necessarily fall behind industry best practices.

More importantly, governments should also not seek backdoors or weakened implementations of encryption or security features in the Internet of Things ecosystem. Given the coming prevalence of connected devices in a variety of sensitive applications, the risks to the

---

[41] *Id.* at 30.
[42] *Id.*
[43] *See* Lauren Cohen, Umit G. Gurun, & Scott D. Kominers, *Patent Trolls: Evidence from Targeted Firms,* HARVARD BUS. SCH. FIN. WORKING PAPER NO. 15-002, 17–24 (Apr. 24, 2016), http://ssrn.com/abstract=2464303.
[44] *See Cisco Global Cloud Index: Forecast and Methodology, 2014-2019 White Paper*, http://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/Cloud_Index_White_Paper.html (last updated Apr. 21, 2016).
[45] *See* Report, *Don't Panic. Making Progress on the "Going Dark" Debate*, BERKMAN CENTER FOR INTERNET & SOCIETY 13 (Feb. 1, 2016), *available at* https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf

public from anything less than the most robust protections for the Internet of Things are too great. Instead, the government, particularly law enforcement and regulatory agencies most concerned with protecting the public, should encourage the adoption and use of the best commercial encryption implementations and security practices available.

D. Infrastructure challenges and development

As NTIA reviews the key technological and policy issues affecting the deployment of IoT, NTIA should consider how the nation's telecommunications infrastructure can support the exponential demand for data that IoT will bring. IP traffic is projected to grow three-fold from 2014 to 2019, representing an annual growth rate of twenty percent.[46] In addition, mobile data traffic is projected to grow seven-fold from 2014 to 2019, for an annual growth rate of forty-seven percent.[47] Much of this growth will come from connected devices.

1. Spectrum and Business Data Services

Carriers are already planning how they can deploy 5G technology in the next few years to keep up with demand for mobile devices. As consumer demand for data from mobile phones and IoT devices intensifies, carriers will need to densify their networks. Carriers will have to deploy more antennae and towers, but they will also have to deploy tens of thousands of small cells to supplement existing macro sites in areas of high demand. Carriers need backhaul to connect these additional facilities to their networks.

Business data services (BDS), also known as "special access," are a crucial component of backhaul and network densification because they provide dedicated transmission lines. For example, competitive wireless carriers often use special access circuits to connect towers to their networks. Competitive wireline providers also use special access circuits from incumbents to connect their business enterprise customers. However, the current, highly concentrated market for BDS has the potential to slow down and raises costs of IoT adoption. The high costs that competitive carriers pay to the incumbents may artificially delay densification and deployment of new facilities due to the anti-competitive pricing of BDS backhaul connections.

Fortunately, after over a decade of delay in a proceeding to review the regulatory regime for BDS, the Federal Communications Commission (FCC) is finally moving ahead by

[46] *VNI Forecast Highlights*, CISCO.com, http://www.cisco.com/web/solutions/sp/vni/vni_forecast_highlights/index.html (last visited May 26, 2016).
[47] *Id*.

considering new rules. This follows on the largest data collection effort that has occurred in the history of the agency.[48] After compiling a comprehensive analysis of the BDS market, the FCC has proposed new long-term, technology-neutral rules for packet-based BDS, including IP-based Ethernet services.[49] The FCC is currently accepting public comments on a new framework to regulate BDS based on determinations of whether markets or products are competitive. The Commission concluded an investigation into certain Incumbent Local Exchange Carrier (ILEC) terms and conditions, deeming unjust and unreasonable "all or nothing" provisions, shortfall penalties, and unreasonable early termination penalties.[50]

CCIA has supported the FCC in its pursuit of fostering competition in the special access market because it will speed deployment of next generation networks. This market represents at least $45 billion per year,[51] yet seventy-three percent of locations are served by just one incumbent without another facilities-based competitor.[52] The FCC's action will help facilitate competition where there are currently bottlenecks in access to networks. Competitive infrastructure providers will be able to build out their networks to new areas and compete head-to-head with incumbents. The FCC's action also has the potential to drive down costs for consumers and businesses that utilize high-capacity broadband lines. If businesses have a real choice for high-capacity circuits like BDS then they will be more likely to save money, which they can allocate to developing new products and services, which can also help foster the advancement of IoT.

2. Ensuring an open Internet for the Internet of Things

The proliferation of IoT devices will require more data, placing additional strains on telecommunications networks. This could present an opportunity for throttling and network management practices that could threaten the principles of openness and neutrality that have been cornerstones of the Internet's incredible success. CCIA has long advocated for open networks, and it pushed for strong open Internet rules before the FCC released its Open Internet

[48] *AT&T Corp. Petition for Rulemaking to Reform Regulation of Incumbent Local Exchange Carrier Rates for Interstate Special Access Services*, WC Docket No. 05-25, RM-10593, Order and Further Notice of Proposed Rulemaking, 27 FCC Rcd. 16318 (2012) (*Data Collection Order* or *Special Access FNPRM*).

[49] *See Business Data Services in an Internet Protocol Environment*, WC Docket No. 16-143; *Special Access for Price Cap Local Exchange Carriers,* WC Docket No. 05-25, Tariff Investigation Order and Further Notice of Proposed Rulemaking, FCC 16-54, (rel. May 2, 2016) [hereinafter "Further Notice"].

[50] *Id.* at ¶ 88.

[51] *Id.* at ¶ 44.

[52] *Id.* at ¶ 181.

rules in 2015.[53] Similarly, the principles of a free and open Internet are central to responding to the increased bandwidth demands from IoT. The FCC's non-discrimination, no-blocking, and no paid-prioritization rules will help preserve an open Internet, and they will ensure that startups and other companies will have the certainty needed to invest and innovate with IoT devices and services.

VI. Conclusion

NTIA's Request for Comment frequently focuses on the *potential* of the Internet of Things. Nascent IoT technologies and services need to be nurtured for the United States to successfully realize that potential. CCIA encourages NTIA to keep the substantial, economy-wide benefits of IoT in mind when developing recommendations for government roles in the space in its forthcoming Green Paper. As standards, regulations, and legislation are considered, principles of openness, competition, and flexibility should characterize government activity with respect to the Internet of Things to best promote its advancement and innovation.

June 2, 2016

Respectfully submitted,

Bijan Madhani
Public Policy & Regulatory Counsel
Computer & Communications Industry Association
900 17th Street NW, 11th Floor
Washington, D.C. 20006
(202) 783-0070

[53] *See In the matter of Protecting and Promoting the Open Internet*, GN Docket No. 14-28, Report and Order on remand, Declaratory Ruling, and Order (released Mar. 12, 2015); *see generally* Comments of the Computer & Communications Industry Association (CCIA), GN Docket No. 14-28 (filed July 15, 2014).