Before the
Department of Commerce
National Telecommunications and Information Administration

In the matter of	
Benefits, Challenges, and Potential Rules for the Government in Fostering the Advancement of the Internet of Things	DOCKET NUMBER 160331306-6306-01

Comments on NTIA Green Paper on IoT

Sam Lowry
239 Sea Cliff Ave
San Francisco, CA

March 13, 2017

Table of Contents

Before the
Department of Commerce
National Telecommunications and Information Administration

In the matter of	
Benefits, Challenges, and Potential Rules for the Government in Fostering the Advancement of the Internet of Things	DOCKET NUMBER 160331306-6306-01

Comments on NTIA Green Paper on IoT

I. NTIA's Role re IoT Policy

The Green Paper begs the question of the appropriate role for NTIA regarding IoT policy.

The paper itself from section to section has different tones as if written by different authors. Generally it reads like a comment summary without doing a literature review or referencing primary research by agencies such as NIST or DHS. It does not offer an intellectual contribution to this subject. It does not draw conclusions based on the extensive submissions in the record, information produced by and in front of other agencies, or other expert agencies. The paper contradicts itself, at one point stating that "IoT is different" and then later stating "there is a lack of agreement from commenters on the subject of privacy that IoT is different." The paper too quickly cites to a comment of a stakeholder as if the proposition presented is true. Where commenters express different views, the paper too quickly throws up its hands and says "there are differences of views that we can't resolve." It limits itself to comments without engaging in a literature review.[1] For example, after the previous comment period closed, but before this paper was issued, the Broadband Internet Technology Advisory Group issued its paper *Internet of Things and Privacy Recommendations* (Nov. 2016),[2] which reflects the consensus position of its 32 members, many of which commented on their own in this proceeding. The consensus work of

[1] This is not an APA regulatory proceeding; NTIA is not limited to the comments before it. NTIA can engage in a review of the expert IoT literature.

[2] *Internet of Things and Privacy Recommendations,* BITAG (Nov. 2016), http://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf

BITAG is in stark contrast to NTIA's conclusion that "commenters were divided"[3] and should have been reflected in the paper.

Too often NTIA pre-determines outcome before considering issues. NTIA's multi-stakeholder process has become its hammer and every policy issue has become a nail.[4] The multi-stakeholder process may have been compelling for internet governance. In that context it makes sense that the process should reflect outcome; that the process of building governance should reflect the outcome of internet governance. This does not mean that this solution is appropriate out of context in areas of cybersecurity, privacy, copyright, or communications infrastructure.[5] Indeed, at some point the chanting of the multi-stakeholder process becomes incoherent.

A role proposed for NTIA was coordination of USG work, but, as discussed below, there is a dearth of evidence in the Green Paper that NTIA is coordinating much less even acknowledging the roles of the other expert agencies. NTIA even goes so far at one point as to suggest that it "developed" the Internet. NTIA appears to be duplicating the work of other agencies. FTC is well positioned to handle privacy and security issues. DHS is exploring security issues. FCC is handling communications infrastructure. DoT is addressing communications between vehicles. NIST is addressing standards.

Given all this, it's not clear what is the appropriate role of NTIA with regard to IoT[6] or whether this paper is needed. The Green Paper should either be substantially rewritten or abandoned.

II. A Working Definition of IoT is Instrumental for a Coherent Policy Discussion

DoC's conclusion that a definition of IoT would be *hard* and therefore should be avoided, is weak.[7] This is particularly weak given that NIST and other experts[8] have provided extensive consideration of

---

[3] Green Paper at 30.

[4] Green Paper at 2.

[5] In support of the multi stakeholder approach, NTIA cites to a 2003 White House directive directing private sector and government to work together voluntarily. Green Paper at 11. It has become painfully clear that this approach has failed. From the IoT DOS attacks to Teddy Bears monitoring the conversations of children, it is clear that we have a market failure. IoT companies lack appropriate incentives to ensure privacy and security. At the recent NANOG 69 conference, members of the community confronted the reality that the failure of industry to act on security puts the USG in a position that it must act. DHS has a task force working this issue. Policy solutions may necessarily look different than the endless process of Internet governance and more like prescribed requirements and certifications.

[6] NTIA has a specific role regarding spectrum management. As numerous commenters noted, the need for more spectrum is vital for the growth of IoT (as well as communications in general).

[7] Green Paper at 5.

[8] See Comments of the Association of Automatic Identification and Mobility at 3 ("That said several international groups are grappling with this very topic. ISO/IEC JTC WG10 as a working group is dedicated to this endeavor as is the ITU-T. The best approach is to join these groups and use the internationally agreed definitions which will be by design slightly behind the development curve. ")

definitions.[9] As NIST stated, "A composability model and vocabulary that defines principles common to most, if not all networks of things, is needed to address the question: “what is the science, if any, underlying IoT?”"[10] As the IEEE stated, "having a sound definition that addresses all the IoT’s features can facilitate a better understanding of the subject, lead to further research and advance our understanding of this emerging concept."[11] As CISCO states, "'words matter,' and when talking about something as broad and diverse as “IoT” it really does indeed matter. It matters because correctly defining what you are speaking about, and to whom, will help to drive towards the right area of focus when describing IoT security."[12]

In order to have an articulate discussion of IoT, it is necessary to have some notion of what it is that we are discussing. It would also be helpful to have a more robust description of IoT so as to understand how IoT impacts policy issues. For example, in the infrastructure section, a description and diagram would be warranted showing how IoT impacts the network. This will help frame consideration of policy issues.

III. The IoT Ecosystem Highlights the Importance of Network Neutrality

The NTIA Green Paper highlights the need for Network Neutrality.[13] Core principles of Network Neutrality include (a) Permissionless Innovation (b) Transparency and (c) Open Platforms. The IoT ecosystem is an environment of many small innovative firms developing niche solutions to meet needs. One product solves medical needs. Another product contributes to the fitness crazy. Another product is sensornet detecting fires. Yet another is a vehicle product contributing to traffic management. There are so many diverse firms innovating and creating cool projects that need an open platform upon which to build.[14] The transaction cost of returning to the old AT&T model[15] of having to ask AT&T permission

---

[9] *See also* FTC Staff Report, Internet of Things: Privacy & Security in an Interconnected World (Jan. 2015).

[10] Jeffrey Voas, Network of 'Things', NIST Special Publication 800-183 at 1 (July 2016); See also J. Voas, Network of Things, PPT.

[11] Towards a Definition of the Internet of Things (IoT), IEEE Internet of Things, p. 6 (May 13, 2015), http://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Issue1_14MAY15.pdf

[12] Munawar Hossain, The IoT(s): One Size Does Not Fit All, CISCO Blog (March 3, 2017), http://blogs.cisco.com/security/the-iots-one-size-does-not-fit-all

[13] Green Paper at 13.

[14] See CSTB, Realizing the Info Future p. 30-31 1994 ("the Internet has given rise to a phenomenon in which services of all kinds spring up suddenly on the network without anyone directing or managing their development....Such spontaneous generation of unforeseen yet enormously popular services—which is encouraged by the Internet as a distributed information and communications system—is a constant source of pleasant surprise today and heralds future potential as we move into an era of truly interactive information via the NII."); Tim Berners-Lee, *Weaving the Web*, 2000 ("The system had to have one other fundamental property: It had to be completely decentralized. That would be the only way a new person somewhere could start to use it *without asking for access from anyone else*. And that would be the only way the system could scale, so that as more people used it, it wouldn't get bogged down. This was good Internet-style engineering, but most systems still depended on some central node to which everything had to be connected – and whose capacity eventually limited

to attach devices to the network would fatally harm this market. If an innovator has to develop a different device and application solutions for each different Internet carrier, the innovation cannot scale and the costs of market entry dramatically rises. Instead, using the IETF model, innovators need transparency from BIAS providers, providing technical information about how their networks work and what protocols and ports will be available. Innovators need to be able to innovate and know that they can bring their products to market in all markets and on all networks. They need to know that they can make the investment to make the next cool thing, and not have that product blocked by the BIAS either to create a barrier to entry in favor of the BIAS' own solution, or to extract rent for the innovator to play on that network.[16] An ecosystem where an IoT business plan can die at the whim of a carrier will chill the market. The innovative information revolution will thrive on an open platform.

IV. NTIA Fails to Demonstrate Interagency Coordination

The paper states as its mission

> "This paper… identifies key issues that can impact the deployment of IoT technologies, highlights potential benefits and challenges, and discusses what role, if any, *the U.S. Government*, particularly the Department of Commerce, should play in this evolving landscape." (Page 1)

Commenters agree that "coordination of federal agencies is essential."[17]

Yet the paper launches into a myopic discussion of IoT considerations that presumes that DoC is the only actor and that DoC invented the Internet. If this is a consideration of the policy approach of the USG, then the paper needs to reflect the full work and responsibilities of the USG, giving full consideration of the work of NIST,[18] DHS,[19] FTC,[20] NSF,[21] NSA,[22] FCC[23] and others.[24] Time and again the paper positions

---

the growth of the system as a whole. I wanted the act of adding a new link to be trivial; if it was, then a web of links could spread evenly across the globe.")

[15] *Hush a Phone Corporation v US*, 238 F.2d 266 (DC Cir. 1956); *Use of the Carterfone Device in Message Toll Telephone Service; Thomas F. Carter and Carter Electronics Corp., Dallas, Tex. (Complainants), v. American Telephone and Telegraph Co., Associated Bell System Companies, Southwestern Bell Telephone Co., and General Telephone Co. of the Southwest (Defendants)*, Docket Nos. 16942, 17073, Decision, 13 FCC 2d 420 (1968) (*Carterfone*), *recon. denied*, 14 FCC 2d 571 (1968).

[16] See, e.g., BITAG: VoIP Impairment, Failure, and Restrictions 2014; Glasnost: Results from tests for BitTorrent traffic blocking. (" Almost 100,000 users from locations around the world have used our tool, Glasnost, to test whether their BitTorrent traffic is being manipulated. On this page, we present preliminary results from these tests. The tests were conducted between March 18th, 2008 and January 27th, 2009. "); AT&T blocks image-sharing site, sparks net neutrality row, CW 7/27/2009; Cable Firms Faulted For Restrictions On Internet Service Washington Post June 2002 ("In a filing with the Federal Communications Commission, the companies say that in the subscriber agreements of major cable Internet providers, there are prohibitions on the use of private corporate networks that allow employees to work from home; restrictions on adding hardware such as servers and game boxes to the networks; and clauses that reserve the right to restrict access to certain bandwidth-intensive sites, such as those for online gambling.")

[17] Comments of ACT at 3; Comments of Association of Global Automakers at 3 ("A principal goal of this leadership should be avoiding a patchwork of different federal and state standards for automated technologies.")

[18] See, e.g., Jeffrey Voas, Network of 'Things', NIST Special Publication 800-183 (July 2016).

DoC as the only actor in this space.

A. DoC's role

> Page 14: "The Department has a longstanding approach to encouraging innovation in new technologies, while taking steps to address policy matters in a proactive, multistakeholder manner. We have approached emerging market trends and technologies with restraint and an eye toward allowing new entrants room to experiment and mature before they encounter significant government intervention. *These guiding principles worked well as the Internet developed*…"

The Department did not develop the Internet. As DoC knows well, the Internet was a project of DOD ARPA, starting in the 1960s. In 1985, NSF entered and added NSFNET. NSF privatized NSFNET in 1995. FCC's Computer Inquiry policy, core to Internet development, dates back to 1966. DOC's entrance was three decades after the start of the Internet and was focused primarily on Internet governance issues. If the mission of this document is to examine USG IoT policy and approach, DoC would do well to avoid such myopic statements.

> Page 41 "The Department will continue to work with its interagency partners to ensure the development of policy that fosters IoT innovation and protects the rights and safety of individuals."

NTIA needs to provide information about how it has and will be working with other agencies. Given the dearth of references to any other agency other than DoC, it does not appear that DoC has been working with its "interagency partners." Indeed, it appears that DoC is duplicating the efforts of other agencies.

B. Labor

> Page 50 " the Department will need to prepare U.S. workers for"

---

[19] See Securing the Internet of Things, DHS, https://www.dhs.gov/securingtheIoT; Strategic Principles for Securing the Internet of Things.

[20] See, e.g., FTC Staff, "Internet of Things: Privacy and Security in a Connected World" (Federal Trade Commission, January 2015); Workshop The Internet of Things: Privacy and Security in a Connected World November 19, 2013; Press Release, FTC, FTC Seeks Input on Privacy and Security Implications of the Internet of Things (Apr. 17, 2013). See also Internet Association at 7 ("Since the late 1990s, the FTC has served as the nation's de facto data protection authority.")

[21] Internet of Things, NSF, https://www.nsf.gov/eng/iip/sbir/topics/IoT.jsp

[22] See The Internet of Things, The Next Wave, NSA (2016), https://www.nsa.gov/resources/everyone/digital-media-center/publications/the-next-wave/assets/files/TNW-21-2.pdf

[23] Disability Advisory Committee Recommendation to the Commission on Internet of Things, Dec. 6, 2016, https://apps.fcc.gov/edocs_public/attachmatch/DOC-342526A1.pdf

[24] See, e.g., Critical Infrastructure and the Internet of Things, Federal Law Enforcement Training Centers, https://www.fletc.gov/critical-infrastructure-and-internet-things; The Internet of Things: Challenges and Opportunities, DipNote Blog, US Dept of State, Nov. 2, 2016, https://www.humanrights.gov/dyn/11/the-internet-of-things-challenges-and-opportunities/; DoD Policy Recommendations for the Internet of Things, December 2016, http://dodcio.defense.gov/Portals/0/Documents/Announcement/DoD%20Policy%20Recommendations%20for%20Internet%20of%20Things%20-%20White%20Paper.pdf?ver=2017-01-26-152811-440

DoC fails to explain why it should be the Department "preparing US workers," as opposed to the Department of Labor,[25] the Department of Education, state governments, or industry efforts.[26] DoC fails to provide information on how it has coordinated with those other agencies on this issue, or what work other agencies and state governments are engaged in.

C. Communications Infrastructure

The section on broadband infrastructure makes no mention of, or indication of coordination with, the FCC.[27] FCC has jurisdiction over the communications infrastructure element of IoT, including local network (unlicensed spectrum, device certification); access network (mobile access, wireline access); backhaul (business data services); and backbone. In addition, NTIA makes no mention of Dept. of Transportation V2V communication proceeding.[28]

V. IoT Poses a "Subtler and More Far Reaching Means of Invading Privacy"

As DoC stated "IoT is different."[29] It is different in terms of scope, scale, and stakes. IoT is pervasive and ubiquitous. It is monitoring, measuring, and surveilling every detail of every aspect of our lives everywhere. As Justice Brandeis warned in 1928, technology evolves to "subtler and more far reaching means of invading privacy."[30] Surveillance has become the normal state of our lives, with IoT devices generating data for ourselves, for the service provider, for the data customers of the service provider, for law enforcement who accesses the data, and for the unauthorized who breach poor security. This data reveals every detail of our lives.[31] As BITAG stated in its recent paper:

---

[25] See Booz Allen Hamilton Comments 2016 at 15 (noting DoC's partnership with the Department of Labor).

[26] CISCO Comments to NTIA 2016 at 28 (discussing CISCO certifications efforts designed to "lead the charge" in educating the work force).

[27] Commenters repeatedly pointed to "numerous proceedings before the FCC." See Competitive Carrier Association Comments to NTIA 2016 at 5; WiFi Alliance at 1 ("NTIA should continue to work with the Federal Communications Commission.")

[28] Federal Motor Vehicle Safety Standards: Vehicle-to-Vehicle (V2V) Communications, Advance Notice of Proposed Rulemaking, 79 Fed. Reg. 49,270 (August 20, 2014).

[29] Green Paper at 3. See also BITAG paper at i ("Although consumers face general security and privacy threats as a result of any Internetconnected device, the nature of consumer IoT is unique in that it can involve non-technical or uninterested consumers, challenging device discovery and inventory on consumer home networks as the number and variety of devices proliferate, impacts on the Internet access service of both the consumer and others that run on shared network links, and effects on other services in that when IoT devices are compromised by malware they can become a platform for unwanted data traffic – such as spam and denial of service attacks – which can interfere with the provision of these other services. ")

[30] *Olmstead v. United States*, 277 U.S. 438 (1928)

[31] See EFF Comments to NTIA at 2 ("Consumer devices that are and will become part of the Internet of Things are designed to collect data on a near-constant basis and share that data broadly—not only with the consumer, but with other devices, with social media, with the manufacturer, with data aggregators, and with known and unknown third parties. In fact, a recent Hewlett Packard study found that 90 percent of IoT devices collected at

> Potential issues contributing to the lack of security and privacy best practices include: lack of IoT supply chain experience with security and privacy, lack of incentives to develop and deploy updates after the initial sale, difficulty of secure over-the-network software updates, devices with constrained or limited hardware resources (precluding certain basic or "common-sense" security measures), devices with constrained or limited user-interfaces (which if present, may have only minimal functionality), and devices with malware inserted during the manufacturing process. [32]

The privacy and security threats posed by the IoT are unprecedented. Even while this paper is out for comment, reports of privacy and security consternations eroding trust continue to pour in.[33] Reports indicate how the CIA and the USG has used IoT devices to pervasively invade the privacy of everyone.[34]

Privacy is one of the foremost concerns of the IoT. As has been repeatedly stated from Ben Franklin and the US Postal Service to modern networking, for communications networks to succeed, individuals must trust the system.[35] Without trust, consumers will avoid and abandon services, and adopt behaviors to protect their own information.[36] Trust in the systems that leads to success of the industry will place the

---

least one piece of personal information via the device, the cloud, or its mobile application.3 This treasure trove of data will prove irresistible for marketers, hackers, law enforcement, and insurance companies. Thus, its collection presents serious risks to security and privacy— at both the individual and societal level."); Brian Fung, Here's the scariest part about the Internet of Things, Washington Post (Nov. 19, 2013), https://www.washingtonpost.com/blogs/the-switch/wp/2013/11/19/ here's-the-scariest-part-about-the-internet-of-things.

[32] BITAG at ii.

[33] *See, e.g.,* Luke Cooper, Millions of Private Messages Between Parents and Kids Hacked in Cloud Pets Security Breach, HuffPo (Feb. 28, 2017), http://www.huffingtonpost.com.au/2017/02/28/millions-of-private-messages-between-parents-and-kids-hacked-in/; Dan Graziano, How to Make Sure Your Vizio Smart TV isn't Spying on You, CNET Feb. 7, 2017, https://www.cnet.com/how-to/disable-vizio-smart-tv-spying/; John Leyden, *We Found a Hidden Backdoor in Chinese Internet of Things Devices - Researchers*, The Register March 2, 2017, https://www.theregister.co.uk/2017/03/02/chinese_iot_kit_backdoor_claims/ ("The vulnerable firmware is present in almost all dbltek GSM-to-VoIP devices, a range of equipment mostly used by small to medium size businesses, it claims. Trustwave researchers claimed they had found hundreds of at-risk devices on the internet.").

[34] *See* Wikileaks embarrasses the CIA, The Economist (Mar. 11, 2017), http://www.economist.com/news/united-states/21718562-agency-which-exists-find-out-secrets-fails-keep-them-wikileaks-embarrasses; Hannah Kuchler, The Internet of Things: Home is Where the hackers are, Financial Times (March 10, 2017), https://www.ft.com/content/cb880bc2-057c-11e7-ace0-1ce02ef0def9

[35] CISCO Comments to NTIA 2016 at 22 ("end users must trust that their data is being securely transmitted"); Written statement of Kevin Werbach, Associate Professor of Legal Studies & Business Ethics, The Wharton School, Hearing on ECPA Reform and the Revolution in Cloud Computing House Judiciary Committee, Subcommittee on the Constitution, Civil Rights and Civil Liberties September 23, 2010 at 8 ("A smooth transition to cloud computing requires users to continue feeling a sense of trust online."); Paul Starr, The Creation of the Media (2005) (discussing how Ben Franklin recognized the necessity of individuals trusting the postal service for the growth of the country and the economy). *See also* FTC, Staff Report, Internet of Things: Privacy & Security in a Connected World, at 55 (Jan. 2015) ("FTC Staff Report"), https://www.ftc.gov/system/files/documents/reports/federal-trade-commissionstaff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf;

[36] Pew Research Center, Public Perceptions of Privacy and Security in the Post-Snowden Era, at 3 (Nov. 12, 2014), http://www.pewinternet.org/files/2014/11/PI_PublicPerception sofPrivacy_111214.pdf; Acquity Group, The Internet of Things: The Future of Consumer Adoption, at 6 (2014), http://quantifiedself.com/docs/acquitygroup-2014.pdf

USA at an economic advantage, and USG firms can thrive.

The concern for IoT and privacy has become particularly acute now that the FCC has abandoned its role in protecting the privacy of concerns. As experts have testified to the FTC, traffic generated by IoT devices can provide ample and detailed information *to ISPs* about customers.[37] When traffic is transmitted, where traffic is transmitted, and how much traffic is transmitted provides an ISP a tremendous amount of information about its subscribers without ever examining the content of those communications. That privacy invasion can be highly intrusive. Chairman Pai stated that the goal of the FCC is that there be uniform privacy protections across the USG. But by abandoning the FCC's role, and the lack of FTC jurisdiction over common carriers in any capacity,[38] the FCC has left a void where no agency has oversight.[39] The incentive and ability to abuse this position is tremendous on the part of ISPs.

DOC appears to dismiss the well established concern for privacy and IoT by stating "commenters were divided on whether IoT presents novel privacy challenges"[40] and "*Several* commenters argued that there are no new privacy issues related to IoT"[41] and then citing to *two* commenters who argue that privacy is no big deal. Two commenters is not "several" and it is not the mark of a divided debate. DoC starts with the premise that IoT is different, and it is. As the Internet Association stated "*there is a broad consensus* that it marks a sea change in the volume, velocity, and variety of data on the network (the so called “Three Vs” of big data), as well as the sources of that data."[42] The privacy concerns of IoT were well documented in testimony during the workshops, in submissions, and by FTC papers.[43]

Notions of self-regulation in privacy and security have evaporated.[44] BITAG presents a series of best practices for IoT but BITAG provides no evidence that firm’s incentive to comply with those best practices will be any different than incentives for security and privacy in the past. Firms have strong incentives to gather every bit of data they can access (needed or not) and minimal incentives to protect that data. USG has engaged in a "light handed regulatory" approach to privacy for almost two decades.

---

[37] See, e.g., Public Knowledge Comments at 13; Paul Ohm, The Rise and Fall of Invasive ISP Surveillance, 2009 U. Ill. L. Rev. 1417, 1423.

[38] FTC v AT&T, 9th Cir Aug. 29, 2016.

[39] Chairman Pai testified before Congress that Sec. 222 is still enforce. See 47 U.S.C. s 222 (Customer Proprietary Network Information); Oversight of the Federal Communications Commission, Senate Commerce Committee Hearing (March 8, 2017), http://www.commerce.senate.gov/public/index.cfm/hearings?ID=B9D3B299-E3CC-480A-B09B-1DEF0512A57C. First, Section 222 privacy protections only apply if broadband internet access service providers fall under title II, which Chairman Pai has indicated he wishes to repeal. Second, Sec. 222 merely provides protection for subscriber information; it offers no protection for the invasive information that can be acquired by monitoring subscriber activity and traffic.

[40] Green Paper at 30.

[41] Green Paper at 31.

[42] Internet Association at 5 (emphasis added).

[43] FTC Staff, “Internet of Things: Privacy and Security in a Connected World” (Federal Trade Commission, January 2015).

[44] Hannah Kuchler, *The Internet of Things: Home is Where the hackers are*, Financial Times (March 10, 2017), https://www.ft.com/content/cb880bc2-057c-11e7-ace0-1ce02ef0def9 (quoting Pedro Abreau, Chief Strategy Officer, ForeScout, "it is a “myth” that manufacturers will be able to solve the security problem.").

The result has been the present environment of perpetual surveillance and privacy compromise.[45] The FCC's recent rolling back of privacy protections is a step exactly in the wrong direction. In order to address these concerns, industry must pursue privacy and security best practices and the USG and other authorities must pursue education, procurement that drives demand, policy including FIPPS[46] and certification, and enforcement.[47]

VI. Avoid Starting Assumptions Regarding USG Involvement

"Commenters have urged the U.S. Government to avoid over-regulation…"[48] This is a cliché. Nobody wants "over regulation." The goal of everyone engaged is the success of America's highly successful technology industry. The question is how do we get there. Positing bogey-men does not get us to a solution and presupposes an outcome. Identify the problem. Identify the challenges. Identify the solution.

Conversely on Page 12 NTIA states

> "The Semiconductor Industry Association commented that the "U.S. government should work with industry to establish a long-term national strategy that will enable America to lead the world in IoT ... that promotes key capabilities, including connectivity and interoperability, scalability and security, and complex intelligent analytics.""

And again

> "the U.S. Government will need to maintain its robust advocacy for industry-led approaches"

This is a cliché in the opposite direction, which presupposes a role for the USG. Does the USG really need to robustly advocate for industry-led approaches?? Industry can't advocate for their own industry-led approaches?? What market failure necessitates that the USG do anything in the space? How is the IoT market not functioning such that the USG needs to have any involvement?

Either the USG needs to be involved or not. But this is a question when looking at solutions; it is not a starting position. There must be something that necessitates USG action, not a starting assumption that USG will or wont act.

VII. Line Edits

> Page 7: "This green paper will continue to use the term Internet of Things as an umbrella term to reference the technological development in which a greatly increasing number of devices are connected to one another and/or to the Internet."

---

[45] EFF Comments to NTIA at 4 ("there is insufficient legal protection for privacy in data gathered by IoT devices").

[46] See Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), NIST Special Publication 800-122 April 2010; Privacy Policy Guidance Memorandum, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security, Dec. 29, 2008

[47] See Internet Association at 6 ("These building blocks include encryption technology; industry best practices for transparency in data use practices and data security; and the Federal Trade Commission's time-tested, comprehensive policy and enforcement frameworks.")

[48] Green Paper at 11.

You are conflating application layer devices connecting with network layer connectivity. They are not the same. At the application layer, devices connect[49] and interact with each other as ends to the network. At the network layer, devices "interconnect" (or attach) to the network and communicate OVER the network, not with the network. At the network layer, the device is not interacting with the network; the device is not communicating with routers and switches (other that providing the destination address); the network is carrying the device's communication traffic to its destination, which is another device or application service.

> Page 9: "Wearable fitness and health monitoring devices and network-enabled medical devices are expected to transform health care, according to the Direct Marketing Association"

This is where the Green Paper reads particularly like a bad comment summary. An authority the impact of health devices would be an expert in the field of health,[50] not the DMA. No disrespect to DMA – their opinion is valid. But DoC needs to cite to the proper authorities for its propositions. The experts for fitness and health would be fitness and health experts.

> Page 10: "For example, according to the Future of Privacy Forum, sensors on roads and in traffic signals can allow for dynamic toll pricing and traffic control to decrease congestion"

Again, the authority for transportation is not FPF. No disrespect to FPF; they have a valid voice in this area, particularly when transportation impacts privacy. But I am sure FPF cited to authorities in the field, not to themselves.

> Page 11: " The U.S. Government has *long* recognized that…"

You make this claim and then cite to 2015 documents.

> Page 19: "*Many* devices *connect* to the Internet via Internet Protocol addresses (IP addresses)"

ALL devices connect to the Internet via IP addresses some how. Either they are directly addressable on the Internet with their own IP address, or they are addressable on the Internet behind another device (like a NAT box) that has an IP address. If they is no IP address involved, then they are not addressable to the Internet.[51]

Further, a device does not *connect* via an address. A device is *addressable* on a network via an address. To connect, it needs connectivity, like cables plugging into ports and routing tables.

> Page 19: "The system most in use today – Internet Protocol version 4 (IPv4)"

IPv4 is not a system; it is a protocol.

---

[49] See connection: 1. A provision for a signal to propagate from one point to another, such as from one circuit, line, subassembly, or component to another. 2. An association established between functional units for conveying information. Federal Standard 1037c.

[50] See, e.g., Dimitrov, D. V. (2016). Medical Internet of Things and Big Data in Healthcare. *Healthcare Informatics Research*, *22*(3), 156–163. http://doi.org/10.4258/hir.2016.22.3.156; G Schreier, The Internet of Things for Personalized Heath, Studies in Health Technology and Informatics, p. 22-31, Volume 200, pHealth 2014.

[51] See Jeffrey Voas, Network of 'Things', NIST Special Publication 800-183 (July 2016) distinguishing between the "Internet of Things" and the "Network of Things."

> Page 19: " Thus, a key question is what incentives or policy approaches, if any are needed, can help quicken…"

Don't presume outcome. Its possible no USG intervention is needed. If it is needed, that needs to be established first.

> Page 19: " Due in large part to IoT, billions of additional devices – from industrial sensors to home appliances and vehicles – will be connected to the Internet between now and 2025"

In the context of the Ipv6 discussion, this is an overstatement. Not all of these devices will be directly connected to the Internet; not all of these devices will have IP addresses; not all of these devices will have *public* IP addresses. A fitbit does not have an IP address. A Roku box in a home does not have a public IP address.

> Page 20: " "Unlike IPv4, which was relatively simple to implement, IPv6 is more complicated," Krawetz, et al, noted."

Unless you are going to say a lot more about this, you should delete this from this paper and include it in anything your produce about IPv6. This is a superficially misleading comment in this context.

> Page 22: " The Department is championing IPv6 adoption…"

How? By putting out an RFC??? It would appear that NIST has been championing IPv6 for USG adoption.

> Page 24: " protected only by factory-default passwords"

Passwords are part of the problem. Please don't over emphasize something that has been established as not a solution.[52]

> Page 26: " many commenters advocated a *riskbased approach* to understand threats and vulnerabilities"

Meaning what? Explain terms that you introduce.

Respectfully submitted,

Sam Lowry

[52] *See, e.g.,* Karen Scarfone, Murugiah Souppaya, Draft Special Publication (SP) 800-118, Guide to Enterprise Password Management, p. ES-2 NIST (Apr. 21, 2009); Michelle L. Mazurek, Saranga Komanduri, Timothy Vidas, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Patrick Gage Kelley, Richard Shay, and Blase Ur, Measuring Password Guessability for an Entire University, CyLab CMU Oct. 22, 2013. Even a recent FTC CTO challenged common myths about passwords. Lorrie Cranor, FTC CTO, Time to Rethink Mandatory Password Changes, FTC (March 2, 2016).