Karim Farhat
PhD Student

School of Public Policy. 685 Cherry St, NW.
Atlanta, GA 30332-0345

DEPARTMENT OF COMMERCE

National Telecommunications and Information Administration

ODCMO, Directorate for
Oversight and Compliance, 4800 Mark
Center Drive, ATTN: Mailbox 24,
Alexandria, VA 22350–1700.

Subject: The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things
[Docket No. 160331306–6306–01]
RIN 0660–XC024

Executive Summary

The Internet of Things (IoT) is predicted to drive significant growth in technology and related markets. Despite a general agreement on the level of economic potential, rapid expansion of IoT businesses has proved counterproductive in the market, particularly when paired with looming legal and regulatory questions. Drawn by attractive economies of scale and a desire to jumpstart market confidence, many large and small firms have grouped together to create open standards in the license-exempt spectrum band under the guise of alliances, which set the technology requirements and guarantee interoperability of equipment within specific environments. These include, inter alia*:* the Open Connectivity Foundation, the LoRa, AllSeen and Zigbee alliances, etc. In practice, standardization activities remain confined to very specific verticals (from link/physical to application layer) and represent archipelagos of disjointed efforts with complex stacks of technology on separate layers while horizontal development is left redundant as Machine-to-Machine (M2M) standards remain fragmented and non-interoperable between most alliances (IEEE, 2016). Government agencies including the NTIA, FCC, FTC and others may need to provide light-handed regulation in different IoT industries to orchestrate the cacophony of efforts that are delaying a full-fledged deployment. The goal being to limit redundancies, helping provide the much needed user quality assurances (cybersecurity, privacy, device shelf-life assurance, etc.) as well as promoting user educational cyber-practices – a point directly relevant to the National Commission on Cybersecurity. As I illustrate in my comments, light-handed regulation when implemented correctly would neither stymie innovation nor require protectionist trade policies to work. In the following sections, I match the order of questions to

follow my own discourse, combining questions when necessary, then proceed to defend my proposed policy recommendations from an economic, regulatory and security perspective.

General questions

1. Are the challenges and opportunities arising from IoT similar to those that governments and societies have previously addressed with existing technologies, or are they different, and if so, how?

A common understanding of policy change is one where long periods of incremental change are alternated by sudden shifts brought about a catalyzing factor(s). In the IoT case, those factors pertain to ever-more frequent strides of technological expansion and Moore's law (Sabatier & Weible, 2014). Internet industry analyst Larry Downes asserts that while social, economic, and legal systems change incrementally, technology changes exponentially (Downes, 2009). For the most part, the IoT has been amplifying existing concerns, some of them unresolved while others have yet to be addressed. In fact, challenges remain at the order of government policies, market forces and influential institutions that shape actions by social norms and business practices. The IoT does however present us with a window opportunity to reevaluate existing policy and regulatory authority. The challenge is to know when to amend legacy policies and rulemakings and when to replace them altogether while ensuring the new rules foster an environment that is conducive to innovation and sustains trickle-down economic effects across society at large.

a. What are the novel technological challenges presented by IoT relative to existing technological infrastructure and devices, if any? What makes them novel?

The following is a non-exhaustive list of technical challenges and their associated policy implications that have to be resolved to sustain a full-fledged IoT deployment; they include:

- Dynamic spectrum access and spectrum allocation: the need to create the right dynamic spectrum access regime (Thanki, 2013).
- Spectrum allocation choices preceding dynamic access: multiple license-exempt band allocations are needed to foster innovation and disfavor market consolidation and closed environments (Forge, 2016).
- Development of a scalable, distributed and layered architecture: current projects (in iCore and IEEE) are working on models that abstract technological heterogeneity to addresses addition of new devices across applications (Sarkar et al., 2015).
- Mobile edge computing and a full 5G deployment are required for some low latency applications such as networked and driverless cars but also industry automation (Hu et.al, 2015).
- Advancements in predictive algorithm technology, deep machine learning and the required workforce of data scientists to back it up.

- Working access control and data sharing consent policies (Roesner et al. 2014).

2. **What definition to use? The term ‘‘Internet of Things’’ and related concepts have been defined by multiple organizations, including parts of the U.S. Government such as NIST and the FTC, through policy briefs and reference architectures. What definition(s) should we use in examining the IoT landscape and why? What is at stake in the differences between definitions of IoT? What are the strengths and limitations, if any, associated with these definitions?**

Finding the right operational definition will help harmonize the developing IoT environment by affording the required precision not only for business and research efforts but also for legal and policy demarcation purposes. Definitions matter as they help map institutional core beliefs to behavior. A generally accepted commonality between definitions includes the exclusion of desktops, laptops or mobile devices (smartphones & tablets) which are in some architectures used as a backhaul gateway in conjunction with routers and switches. Notable exceptions include the IETF. Their rationale for including computers as another node in the network is based on their separation between interconnected TCP/IP and non-TCP/IP networks on the one hand and ‘things’[1] on the other.

Institutional definitions of IoT emphasize different aspects of the technology revealing their cultural biases; the NIST definition refers to the IoT as cyber-physical systems (CPS) – an area implying a focus on cybersecurity whereas the FTC underscores devices that are “sold to or used by consumers” thereby excluding B2B or M2M communications. Other definitions such as the ITUs or ETSI are simply too vague and open to interpretation. For a more complete account of IoT definitions including architectural requirements refer to Minerva et al. 2015. In their article, Minerva et al. show how from a networking standpoint, the NIST definition refers to a different Internet layer and should be discounted (Minerva et al. 2015 p, 71). IEEE researchers also found that “projects in the IoT space give better definitions and architectural models than the standardization bodies. Unfortunately, the acceptance of these definitions and models is difficult outside of the community that works on a specific project.” This is an understandable notion as projects will have a specific architecture and inclusion/exclusion criteria whereas institutions will tend to be broad in culturally biased. The Internet Society’s definition refers to the extension of network connectivity and computing capability to objects, devices, sensors, and items not ordinarily considered to be computers. These ‘smart objects’ require minimal human intervention to generate, exchange, and consume data; they often have connectivity to remote data collection, analysis, and management capabilities (Internet society, 2015). This definition works as it is focused enough yet leaves the possibility open to the blurring of what is traditionally understood

[1] In an unconventional divergence from their usual purely technical (and sometimes humorous) RFCs, the IETF separated ‘things’ into three categories: people, machine and information. This categorization brings the IETF’s definition closer to the ITU’s by conveying the message that the IoT is a vision with societal implications rather than a technical protocol. I am against such categorizations as they are only bound to add further complexity and would prefer technical demarcations that follow the network layers model.

as a 'computer'. It does not discriminate based on architecture model or leaves much room for interpretation.

16. a. What are the cybersecurity concerns raised specifically by IoT and how are they different from other cybersecurity concerns?

The IoT has many characteristics that make it fundamentally more challenging in terms of standard cybersecurity concerns. This is mainly due to the ubiquitous, interconnected and pervasive nature of full deployment scenarios conjured up in think tanks and startups. First among the list of problems is the monoculture issue, or, the downsides of having a single type of components or operating systems dominate the market. A commonly cited example in technology circles refers to the Windows operating system whereby malicious actors can "tailor exploits [to one operating system] or associated application (Office, Internet Explorer) and be confident that 9 of 10 systems their malicious software encounters will at least be running some version of the software they're targeting" (Security Ledger, 2014). In an IoT-enabled society, threats are greatly amplified, implying more negative network externalities i.e. botnets using lax security of 'things' as a transmission vector to compromise other systems and the whole network loses usability as a consequence. As smart-sensors or microprocessors (Arduino, Raspberry Pi, Adafruit, etc.) with either one way or two-way communication become common commodities with small costs and diverse functionalities, the attack surface will greatly increase.

Second on the list are authentication, access control, updates and self-life issues. Since most IoT nodes won't have a User Interface (UI), automatic 'push' updates with minimal user interaction will be required[2]. However, who will push updates to 'things' once the commodity supplier is out of business? This problem is commonly referred to as IoT device shelf-life or orphan IoT devices. In this case, industry self-regulation brought about institutional norm-setting would be advised as in the following section.

How should the government address or respond to cybersecurity concerns about IoT?

A new cyber environment opens up policy windows for improving the status quo; it is imperative not to recreate the raucous PC security state of the late 90s[3]. In the cost vs. security tradeoff, security always loses in an unregulated market. Homogenous sensor deployment and near identical devices magnify similar vulnerabilities. In their relentless race to find the most cost-viable products, many manufacturers are skimping on security and compromising their user's data in the search for a competitive edge. The network is only as secure as its weakest node and simply advertising for better security is not going to make a difference. A standard preliminary

[2] Although push updates are theoretically less risky than firmware changes are costly to implement and not within reach of the average consumer

[3] Deploying Windows ME or [insert other example] and worrying about security later

approach to regulatory considerations in any industry is to ask whether we should give the carrot or the stick.

The stick solution

Wyndham v. FTC further solidified the agency's position as a digital watchdog that pushes for best-practices, some of which were mentioned in their 2015 IoT report[4]. A failure to implement reasonable[5] security is now considered a violation of the FTC act[6]: guided by their mandate to protect consumer affairs, the FTC is setting the de facto minimum cybersecurity good practice to be followed by threatening non-compliant entities with an enforcement action against "unfair and deceptive practices" and the accompanying bad press[7]. Although the FTC is well within their mandate and their approach is valid for the time being, the agency may find itself using indirect and borderline deceptive legal techniques to fulfill their mandate. The FTC may also prove to be severely understaffed and some companies, in their race to releasing a minimally viable product, may not even make claims of selling secure solutions – which would invalidate the FTC's position.

The carrot approach

If a private sector consumer report alternative is to be considered, the implication could mean using monetary incentives for products with a higher security rating in the form of tax breaks for meeting ISO or industry specific security standards. Mandatory certifications through data security legislations (such as the Euro NCAP ratings) are to be avoided in order not to fall into the trap of market exclusions.

- Independent safety ratings organizations are a mixed-bag however: Testing and reporting organizations such as Underwriter Labs certifies, trains industry and performs audits but lacks the transparency needed when it comes to disclosing their security standards. Independent researchers such as the iamthecavalary.org group have sound ideas, however, they might not get sufficient inertia for market adoption.
- Another solution within the NTIA's reach is to encourage open source software adoption (for instance the AllSeen IoT Standard by the Linux foundation) through exclusive government procurement. Private sector companies concerned with complete vertical integration like Apple, are heavily incentivized to lock-down their devices from 3rd party

[4] FTC, 2015 Internet of Things, Privacy and Security in a Connected World
[5] Wyndham Hotels were certainly culpable as the company had a privacy policy designed to attract customers concerned about data privacy yet failed to uphold that promise even after three public warnings (court ruling).

[6] 15 U.S. Code § 45 - Unfair methods of competition unlawful; prevention by Commission
[7] Companies face more than a mere 'slap on the wrist' as enforcement actions can incur reputational losses on top of monetary due to mandatory compliance with a 20 year long audit no company is going to want to be made to look bad.

open source firmware and won't allow users to tamper with their own devices. The FCC is following the same trend: their concern about transmit power requirements is making them push to lock down router firmware alteration: such policies are not IoT friendly.

What are the novel policy challenges presented by IoT relative to existing technology policy issues, if any? Why are they novel?

Institutions in the broader Internet governance regime complex have been recently addressing the rise in salience of the IoT by forming working groups, drafting white papers, and asking the 'hard' questions [ITU: (Brown, 2015) ISOC: (Rose et. al 2015) OECD: (Paltridge & Hernandez, 2015) IEEE (Minverva et. al, 2015) etc.]. Again, most policy challenges presented by the IoT pertain to existing issues with added layers of complexity. Those challenges resurged as a result of enabling ICT developments ('big data', cloud computing and M2M communication), and increasing numbers of stakeholders (users, private companies and interest groups), as well as amplifying existing concerns in cybersecurity, privacy and innovation policy.

Can existing policies and policy approaches address these new challenges, and if not, why?
15. What are the main policy issues that affect or are affected by IoT? How should the government address or respond to these issues?

A- Innovation policy

The U.S. government played a historical role among others in shaping today's Internet by allowing independent institutions with transparent processes such as the IETF to develop working standards. Internet innovation advocates from Vinton Cerf to Shane Greenstein agree that the open Internet generated enormous economic added value thanks to the permissonless innovation environment that permeated its outlook: distributed, interoperable and copyright exempt TCP/IP meant freedom to tinker and experiment without having to seek approval from regulators beforehand. Greenstein affirms that "innovation from the edges emerged under the encouragement of several institutions embedded in U.S. commercial markets and government policy conversations" (Greenstein, 2015 p. 439). This was made possible through a series of soft and hardline policy approaches. With the benefit of hindsight, we can see how a hardline approach may in some cases be necessary as when Section 230 of the Telecommunications Act of 1996 removed ISP liability from their users.

When it comes to innovation, adopting a general policy of forbearance and permissiveness over more precautionary stances is obviously preferable unless empirically proven otherwise by a cost-benefit analysis. Adam Thierer at the Mercatus Center, presents cautionary accounts explaining how 'top-down' regulatory frameworks will stymie innovation and that "permissionless innovation should, as a general rule, trump precautionary principle thinking" (Thirer, 2016). Thierer argues that imposing preemptive regulation on technology needs strong evidence of "actual, not merely hypothesized harm" (Ibid).

Certain harms, however, won't necessarily fix themselves in the market and may require industry-specific intervention:

- Increasing security flaws and privacy concerns[8]
- Constricted transnational data flows (data sovereignty v. safe harbor) especially with the looming European General Data Protection Regulation (GDPR) going into effect in 2018.
- A diffuse buyers' market with little expertise to assess or purchase
- Sellers in a commodities market constrained by the race to a minimum viable product to release early and mark around security best-practices. The free market won't reward good security and we are left with negative network externalities. This implies asymmetric information[9] between buyers who can't tell good security from bad and sellers who all claim their products are secure.

B- Industry regulation

A strong empirical economic rationale must guide any IoT regulatory decision. The free market baseline has been the operating principle of the U.S. telecommunications sector ever since the AT&T divestiture which paved the way for the Internet backbone privatization. 2015 was the year of debating IoT regulation, reports and white papers ranged from ISOC and the OECD to the FTC and US Senate Committee on Commerce, Science and Transportation. The FTC staff Report,[10] concluded *inter alia* that regulating the IoT was to be avoided as setting up a new control regime could stymie American innovation in a nascent industry. The Senate Committee hearing displayed bipartisan support for no regulation two weeks after the FTC report. Citing the government's "light-touch, market-driven approach" as a success in privatizing the Internet backbone, Senate parties agreed without going into specifics that self-regulation was the best way to move forward. Both the FTC and FCC are valid candidates[11] to provide the 'light-touch, market-driven approach'. However, as I describe later, industry stakeholders will need a clearer understanding of where self-regulation, light-regulation (incentives or market mechanisms) will be favored, or if hardline regulation will occur (such as a general data security legislation). Contrary to common political discourse, the right dose of regulation can often be conducive to innovation and act as a freedom safeguard, for despite being born free, markets will not always lead to the most favorable outcomes for the public (Wu, 2010).

C- Legacy infrastructure

[8] Also to be addressed by the National Commission on Cybersecurity.

[9] (one of the many potential causes of a market failure)

[10] Federal Trade Commission. (2015). Internet of Things: Privacy & security in a connected world. *Washington, DC: Federal Trade Commission*.

[11] The FTC for consumer affairs serving enforcement-actions on privacy and security breaches and the FCC for building the market competition environment (through spectrum allocation, power requirements, ISP regulation, etc.)

Commonly cited IoT business reports such as the McKinsey Global Institute[12], raise the issue of bandwidth availability (p, 36, 82). Despite the current projections of a tremendous number of smart nodes on the network[13], the bulk of incoming devices will be low-powered and low-bandwidth. Further, based on the current information economy market dynamic – and even after common carriage regulation under title II[14] - we can expect a continually increasing bandwidth demand to be met with a matching supply from the private sector as long as the incentives to create and consume[15] content on the Internet outweighs the cost to transport it (no 'tragedy of the commons' situation).

D- Data science education

As enormous amounts of data are generated, value propositions are held back by the inability to generate useful optimizing and predictive insights from bulk data brought upon the lack of availability of data scientists. The issue is relevant despite being outside of the NTIA's scope.

E- Anti-trust

Consolidation of alliances in the IoT has different considerations than for the regular Internet and its layers of actors. The latter deals with abuses of market position through consolidation i.e. concerns brought upon content creation and delivery by the same holding company. In an IoT environment, market abuses could occur if data sharing occurs between smart-pacemakers or networked cars manufacturers with insurance companies. Further, revisions of the Sherman and Clayton Acts are needed to fit the current market landscape. This is especially relevant since traditional definitions of a monopoly position (as the power to raise price or exclude competition) no longer applies in complex two-sided network markets (Waller, 2011).

F- Portability and interoperability

These issues are time critical. As social networks become more integrated with the IoT it will become harder for them to adapt to imposed market changes pertaining to data portability. Beyond the privacy and security implications[16] benefits of portability and interoperability are usually addressed from a market competition standpoint. The argument against them is that any entrant platform operator can interoperate with the incumbent players and benefit from their network value thereby undermining the incentive for innovation. The reverse argument however holds true as well: by expanding interoperability, we create the overall network benefits and

[12] IoT: Mapping the Value Beyond the Hype (Manyika et al., 2015).
[13] Based on current standards and protocol developments and with some exceptions
[14] Pro-industry discourse maintains that the universal service fund subsidy mechanism and potential inter-carrier compensation regimes will hinder Internet or IoT deployment.

[15] Targeted advertising models, predictive analytics and cross-merchandising practices sustain the information economy business model because as per the common saying: 'the user is the product'.
[16] Could be resolved by the W3.

expand platform matching capabilities. This held true for interconnecting telephone systems and should hold true for the Internet and IoT as well. The catch is that an entity (government agency or standards body like the W3C) needs to orchestrate and present a valid model.[17]

References

Aronson, J. D. (2016). Shane Greenstein, How the Internet Became Commercial: Innovation, Privatization, and the Birth of a New Network. *International Journal of Communication*, *10*, 3.

Downes, L. (2009). *The laws of disruption: Harnessing the new forces that govern life and business in the digital age*. Basic Books.

Forge S., (2016),"Radio spectrum for the internet of things", info, Vol. 18 Iss 1 pp. 67 - 84

Hu, Y. C., Patel, M., Sabella, D., Sprecher, N., & Young, V. (2015). Mobile Edge Computing—A Key Technology Towards 5G. ETSI White Paper, (11).

Minerva et al., (2015): IEEE Towards a definition of the Internet of Things (IoT) Revision 1, May 2015.

Roesner, F., Molnar, D., Moshchuk, A., Kohno, T., & Wang, H. J. (2014, November). World-driven access control for continuous sensing. In*Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1169-1181). ACM.

Sabatier, P. A., & Weible, C. (Eds.). (2014).*Theories of the policy process*. Westview Press.

Sarkar, C., Nambi, A. U. S. N., Prasad, R. V., Rahim, A., Neisse, R., & Baldini, G. (2015). DIAT: A Scalable Distributed Architecture for IoT.*Internet of Things Journal, IEEE*, *2*(3), 230-239.

Thanki, R. (2013). The case for permissive rule-based Dynamic Spectrum Access.

Thierer, A. (2016). *Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom*. Revised and Expanded Edition Mercatus Center at George Mason University.

Waller, S. W. (2011). Antitrust and social networking. *NCL Rev.*, *90*, 1771.

Wu, T., & Vietor, M. (2011). *The master switch: The rise and fall of information empires*. Vintage Books.

[17] Perhaps through negotiated interconnection rates if micropayments can be made viable.