National Telecommunications and Information Administration
Docket No. 160331306–6306–01
RIN 0660–XC024

INTERNET COMMCERCE COALITION COMMENTS ON NTIA IOT RFC

I. INTRODUCTION

The Internet Commerce Coalition (ICC), a coalition of major Internet companies, including both ISPs and edge providers, applauds National Telecommunications and Information Administration 's (NTIA's) initiative seeking comments on policy principles to guide Internet of Things ("IoT") development, deployment and use, including on ways to head off conflicting, sectorial, agency-by-agency regulation that would stifle growth in this sector.[1]

The ICC supports an NTIA led multistakeholder process to frame the parameters of what government/agencies should do and should not do when addressing the IoT.[2]

The IoT holds significant promise to bring broad societal benefits through efficiencies in managing natural resources, environmental protection, energy usage, manufacturing processes, agricultural production, traffic and auto safety, improved health care, government services, and public safety. At the same time, there are common types of technological functions used in this huge range of sectoral applications. A multistakeholder developed, cross-sectoral approach that offers a baseline analytical framework to guide policy in the area is important for continued IoT innovation and deployment of new services.

II. NTIA SHOULD ESTABLISH PRINCIPLES TO GUIDE THE GOVERNMENT'S APPROACH TO IOT

In addressing safety, security or privacy issues for the IoT, government should first look to self-regulatory and multistakeholder efforts.[3] As the 2012 White House privacy report noted[4], particularly for evolving technologies, these initiatives can address the relevant issues in a more nuanced way and do so more quickly and flexibly than can government regulations. If such an effort is not already under way, government should consider convening one before considering issuing any additional regulations. Furthermore, any regulations that government may ultimately contemplate should be as light-touch as possible in order to preserve existing incentives for innovation in the IoT space.

---

[1] Notice, Request for Comment, NTIA, Docket No. Docket No. 160331306–6306–01 ("NTIA RFC")
[2] NTIA RFC questions 25, 26
[3] NTIA RFC question 17.
[4] *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (Feb. 23, 2012) p. 24 https://www.whitehouse.gov/sites/default/files/privacy-final.pdf (White House Privacy Report).

A. The green paper should encourage the preemption of agency-by-agency, sectorial regulation through the principle of tech neutrality.

Companies in virtually every industry sector are undertaking IoT initiatives. NTIA's "green paper" should head off conflicting agency-by-agency regulation that may stifle economic growth and innovation in the IoT sector. NHTSA, FCC (in its Broadband Privacy NPRM)[5], FTC, FDA, FAA (drones including pursuant to the FAA reauthorization bill[6]), and GSA/DOD procurement rules, and state and local laws are all potential sources of uneven and disjointed sector specific regulation.

Given the siloed regulatory authority of each of these agencies, scenarios could easily arise where two regulated entities (working together on an IoT device or service) are required to undertake incompatible approaches to the device or service deployment because of conflicting regulatory requirements. Two entities developing competing IoT products could be subject to two different set of rules, causing regulatory disparity, fragmentation in both IoT device development and IoT services, and consumer confusion.

For example, NHTSA has auto safety related rules establishing a 12-year data retention requirement for purposes of tracking auto performance over the course of a vehicle's lifetime. Likewise, the FCC has rules applicable to telecom carriers requiring that certain call records be retained for a minimum of 18 months.[7] In contrast, the FTC IoT Report calls for limited customer data retention timeframes[8] as does the White House Consumer Privacy Bill of Rights[9] and numerous privacy bills introduced in Congress.[10] Furthermore, the FCC's Broadband Privacy NPRM has asked if there should be data minimization and destruction mandates for such data.[11]

---

[5] *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Notice of Proposed Rulemaking, WC Docket No. 16-106 (March 31, 2016), "FCC Broadband Privacy NPRM").
[6] S. 2758, H.R. 4441 (114th Congress).
[7] 47 C.F.R. § 42.6.
[8] *Internet of Things, Privacy and Security in a Connected World*, FTC Staff Report, Jan. 2015, pp. iv., vii, 35-37, and 39 ("FTC IoT Report") https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.
[9] Administration Discussion Draft Consumer Privacy Bill of Rights Act of 2015, https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf.
[10] S.1158, Consumer Privacy Protection Act of 2015 , Sen. Patrick Leahy, 114th Congress; H.R. 4517, the Application Privacy, Protection, and Security Act of 2016 (APPS Act), Rep. Hank Johnson, 114th Congress; S. 547, Commercial Privacy Bill of Rights Act of 2015, Sen. Bob Menendez (114th Congress).
[11] FCC Broadband Privacy NPRM, ¶¶ 129, 221, and 230.

The IoT landscape is not limited to devices and systems that communicate within a single traditional category (consumer vs. industrial, public vs. private, device-to-device vs. human interfacing).[12] For example, devices used for vehicle telemetrics may be used for personal purposes by the owner of an automobile for monitoring battery levels or engine status, but the device may also be used by first responders following an accident. NTIA should discourage continuing down the road of siloed regulatory models. Instead, NTIA should develop a forward-looking cross-sectoral approach, rather than leaving other regulators on the course of attempting to shoehorn the IoT into legacy frameworks.

We respectfully request that NTIA head off disparate treatment of IoT by adopting a principle of technology neutrality in privacy and security regulation. NTIA should establish this cross-cutting, technology and sector neutral paradigm based upon existing, tech neutral frameworks like the National Institute of Standards & Technology (NIST) Cybersecurity Framework[13], the 2010 Department of Commerce green paper[14], the White House Privacy Report[15], and the FTC IoT Report[16], which already provide adequate tools to meet new challenges.[17] The framework could leave room for additional safety regulation, for example, but establish a clear set of principles and purposes under which additional requirements would be acceptable.

B. The green paper should include a principle on process outcomes for security and privacy.

The green paper should reiterate the importance of process outcomes that can evolve with security threats, instead of mandating particular security solutions. This approach was used with the NIST Cybersecurity Framework. As with the NIST Cybersecurity Framework, exercises in identifying process outcomes should be accompanied by the identification of security standards developed by standards organizations and industry best practices.[18] This approach allows for recognition that the mechanics and core approaches to security do not vary materially by sector, again emphasizing the first principle of tech neutrality.[19]

---

[12] NTIA RFC question 4.
[13] NIST Cybersecurity Framework, Feb 12, 2014 http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.
[14] *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*, Internet Policy Task Force Green Paper, December 16, 2010, fn. 124, https://www.ntia.doc.gov/report/2010/commercial-data-privacy-and-innovation-internet-economy-dynamic-policy-framework.
[15] White House Privacy Report, p. 24.
[16] FTC IoT Report.
[17] NTIA RFC, question 1b.
[18] *See NIST Cybersecurity Framework*, Framework Core, Informative References pp. 20-35.
[19] NTIA RFC questions 16a. and 16c.

C. The green paper should include a principle establishing that privacy protections must be based upon the sensitivity of information.

NTIA should caution against prescriptive rules for a risk resulting from information emanating from the IoT. Consistent with the FTC privacy framework, information about children, financial and health information, Social Security numbers, and precise geolocation data should be treated as sensitive.[20] However, sensitive information could evolve in the future, just as it has in the FTC framework. Consequently, as noted above, government should defer first to self-regulatory or multistakeholder proceedings, which can quickly and flexibly address existing challenges. Failing that solution, any proposed rules should be as light-touch as possible and reflect the same flexibility inherent in the FTC framework.

D. The green paper should include a principle of flexibility for future use of IoT data.

Many of the new beneficial uses of IoT data arise from the ability to analyze, combine, and share data after it is collected including for purposes that were not initially anticipated at the time of collection.[21] Finally, in this privacy principle, NTIA should recognize the important correspondence between Big Data and IoT, including significant, very beneficial uses of deidentified data in conjunction with the IoT and embrace a de-identification standard that both protects personal privacy and enables innovation.

Use-based restrictions based upon the context of the use and a reasoned risk-based analysis by the company offering the IoT product or service as an alternative to user choice should be an option rather than a top down, blanket regulatory requirement for "informed consent". Consequently, we ask that NTIA provide for a principle allowing for flexibility in innovation that will resolve conflicts with constructs for notice and consent that may not be optimal for devices without a user interface enabling informed consent.

III. The principles should be developed by the Internet Policy Task Force.

The above principles should be developed by the Internet Policy Task Force and proposed to the White House and the Office of Management and Budget (OMB).[22] There should

---

[20] *Protecting Consumer Privacy in An Era of Rapid Change*, at 58-60 (March 2012), ("FTC Privacy Report") available at https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[21] Center for Data Innovation, Daniel Castro & Jordan Misra (Nov. 2013) http://www2.datainnovation.org/2013-internet-of-things.pdf.

[22] NTIA RFC, question 17c.

be a mechanism to ensure that all agencies considering regulation of IoT adhere to these principles.

IV. The Department of Commerce should initiate a dialogue to reduce international barriers to IoT deployment and use.

The current international approach to telecom regulation including on roaming, interoperability, and equipment authorizations should not extend to the IoT. Instead the Department of Commerce should initiate an international dialogue. Such a dialogue would aim to promote cross-border IoT deployment and use through policies that enable seamless cross-border roaming, flexible use policies and equipment processes that allow for interoperability, and voluntary industry led standards.[23] The goal of such efforts would be that IoT devices and services aren't confronted by barriers to the seamless use of the IoT and the need to adopt a country-by-country compliance program.[24]

Respectfully submitted,

/s/

Jim Halpert
Sydney White
Counsel to the Internet Commerce Coalition
DLA Piper LLP (US)
500 8th Street, NW
Washington, D.C. 20004
(202) 799-4441

[23] NTIA RFC questions 20, 21, 23, 24, and 27.
[24] NTIA RFC, questions 20, 27.