NetChoice *Promoting Convenience, Choice, and Commerce on the Net*

Carl Szabo, Senior Policy Counsel
NetChoice
1401 K St NW, Suite 502
Washington, DC 20005
202-420-7498
www.netchoice.org

May 26, 2016
SUBMITTED ELECTRONICALLY
Federal Trade Commission

NetChoice Public Comments to NTIA Request for Comments on the Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things

NetChoice respectfully submits the following comments regarding the National Telecommunications and Information Administration ("NTIA") request for comments on the Internet of Things (IoT).[1]

NetChoice is a trade association of leading e-commerce and online companies, plus thousands of small businesses that rely on e-commerce. We work to promote the integrity and availability of the global internet and are significantly engaged in privacy issues in the states, in Washington, and in international internet governance organizations.

IoT doesn't create a new internet. Nor does it require changing the internet – a system of locally connected networks. Nor does IoT require creating a new regime of internet regulations.

What IoT creates is an amazing landscape for innovation, growth, and development of new technologies and tools. But while IoT may seem like a new landscape, it certainly does not necessitate the creation of new rules or regimes. Under the NTIA's Request for Comments definition of IoT, it is clear that IoT devices already abide by strict rules and regulation.

IoT has been around for more than a decade.[2] The term IoT was first coined in 1999[3] to refer to RFID chips. Since then we have developed IoT devices, even if they don't meet some advocates current interpretation of IoT. With over fifteen-years of development, we have developed rules, regulations, and best practices.

IoT doesn't create a new internet. Nor does it require changing the internet nor does it require creating a new regime of internet regulations.

For example, in 2006 Nokia introduced the "5500 Sport" phone that included a pedometer. Much like a FitBit or Jawbone Up, the 5500 Sport provides a "connection of physical objects, infrastructure, and environments to various identifiers, sensors, networks, and/or computing capability… [and] also

---

[1] NTIA Request for Comments - *The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things* (Docket No. 160331306–6306–01).

[2] Kevin Ashton, *That 'Internet of Things' Thing RFID Journal*, (May 2009) *available at* http://www.rfidjournal.com/articles/view?4986.

[3] *Id.*

encompasses the applications and analytic capabilities driven by getting data from, and sending instructions to, newly-digitized devices and components."[4]

The 5500 Sport operates under regulations from the FCC. Likewise, Nokia privacy policies and terms of service operate under the FTC Act's Section 5 prohibition against "unfair and deceptive trade practices." Moreover, many sectoral laws already apply to devices that could be considered under the auspices of IoT.

An Early IoT Device

Existing Law Already Requires App Connected IoTs to Have Privacy Policies

If an IoT device uses an app for operation, it's already required to have a privacy policy. FTC Section 5, FDA regulation, and state laws like the California Online Privacy Protection Act (CalOPPA),[5] provide regulators with ample authority to compel app developers to build useful and comprehensive privacy policies.

According to the California Attorney General's interpretation of CalOPPA any mobile application that may impact a California consumer that collects personal user data must conspicuously post a privacy policy detailing, clearly and completely, how the application collects, uses, and shares personal data. In effect, all apps are subject to the CalOPPA privacy policy rules. And of course this includes app connected IoTs.

In late 2012, the California AG began taking enforcement actions against apps for not posting privacy policies. The AG sent out a wave of notifications to 100 companies in October 2012, warning app developers to post privacy policies or risk fines as high as $2,500 per app download.[6] The AG then took action against mobile app developers, including Delta Airlines.[7]

FTC statements show the agency believes it has enforcement authority against an app for lack of a privacy policy, or one that fails to disclose material information.[8] And the FTC is aggressively enforcing its authority when it comes to mobile apps not abiding by their privacy policies. In 2013, the FTC took action against Path,[9] Goldenshores Technology, and most recently SnapChat[10] for collecting information outside the scope of the privacy policy. And the FTC settlement with Fandango and Credit Karma

---

[4] [4] NTIA Request for Comments - *The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things* (Docket No. 160331306–6306–01).

[5] The Online Privacy Protection Act of 2003, Cal. Bus. & Prof. Code §§ 22575-22579

[6] Press Statement, *Attorney General Kamala D. Harris Notifies Mobile App Developers of Non-Compliance with California Privacy Law*, California AG Office (Oct. 30, 2012), *available at* http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-notifies-mobile-app-developers-non-compliance

[7] Press Statement, Attorney General Kamala D. Harris Files Suit Against Delta Airlines for Failure to Comply with California Privacy Law, California AG Office (Dec. 6, 2012), available at http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-files-suit-against-delta-airlines-failure

[8] *See e.g.,* Sears Holdings Mgmt. Corp., Docket No. C-4264, File No. 0823099 (Fed. Trade Comm'n Sept. 9, 2009) (decision and order), *available at* http://www.ftc.gov/os/caselist0823099/090604searsdo.pdf

[9] Press Statement, Path Social Networking App Settles FTC Charges it Deceived Consumers and Improperly Collected Personal Information from Users' Mobile Address Books, FTC (Feb. 1, 2013), available at http://www.ftc.gov/news-events/press-releases/2013/02/path-social-networking-app-settles-ftc-charges-it-deceived

[10] Snapchat Inc., Docket No. C-4264, File No. 1323078 (Fed. Trade Comm'n) (decision and order), *available at* http://www.ftc.gov/system/files/documents/cases/140508snapchatorder.pdf

further shows that promises made in privacy policies extend to the security of information transmitted and stored.[11] Clearly, the FTC already has the legal authority it needs to regulate IoT when connected to apps.

EXISTING LAWS ALREADY REGULATE HEALTH RELATED IOTS

The Department of Health and Human Services (HHS) and Food and Drug Administration (FDA) are already involved in the regulation of IoT devices. For example, the FDA issued guidance regarding the regulation and certification of health apps, stating, "The FDA is taking a tailored, risk-based approach that focuses on the small subset of mobile apps that meet the regulatory definition of 'device' and that: are intended to be used as an accessory to a regulated medical device, or transform a mobile platform into a regulated medical device."[12]

Regulation of health apps exists and developers are responding to improve their privacy policies. Likewise, the same can be expected for devices that fall under the category of IoT.

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?

As discussed above, NetChoice believes that IoT does not create a new universe of policy questions or necessitate new regulations.

As seen with the idea of a cell phone that can access the internet, or a pedometer built into that cell phone, we've been living with IoT for more than a decade and already implemented regulations and business practices for IoT. Moreover, businesses have adopted best practices and created privacy policies to which they are liable.

1. A. WHAT ARE THE NOVEL TECHNOLOGICAL CHALLENGES PRESENTED BY IOT RELATIVE TO EXISTING TECHNOLOGICAL INFRASTRUCTURE AND DEVICES, IF ANY? WHAT MAKES THEM NOVEL?

As stated above, we do not believe that there are general policy challenges for IoT. Aside from the new challenges regarding IPv6 and mobile IP addresses (discussed below in Question 24), IoT is simply a new term for a device that access the internet.

IoT doesn't create a new internet. Nor does it require changing the internet – a system of locally connected networks. Finally, IoT does not require creating a new regime of internet regulations.

Moreover, it's clear that IoTs already operate under rules and regulation.

1. C. WHAT ARE THE MOST SIGNIFICANT NEW OPPORTUNITIES AND/OR BENEFITS CREATED BY IOT, BE THEY TECHNOLOGICAL, POLICY, OR ECONOMIC?

Significant benefits stem from IoT. This can include system optimization, increasing internet access, and assisting consumers in achieving greater energy efficiency.

For example, the Nest thermostat allows consumers to better control their home HVAC systems. This means that they can turn off systems when not present and avoid unnecessarily

IoT can provide system optimization, increasing internet access, and assisting consumers in achieving greater energy efficiency.

[11] Press Statement, Fandango, Credit Karma Settle FTC Charges that They Deceived Consumers By Failing to Securely Transmit Sensitive Personal Information, FTC (Mar. 28, 2014)

[12] Food and Drug Administration, Mobile Medical Applications (10/23/13).

using energy. Likewise, with IoT shipping containers, transportation businesses can better optimize routes and identify missing or lost shipments. Finally, IoT is embodied in the ability of smart phone users to access high-speed internet when they might otherwise not have online access.

2. What definition(s) should we use in examining the IoT landscape and why?

Looking to the man who first coined the term "Internet of Things" we suggest using his phrase:

> ***IoT means "a ubiquitous ad hoc open network of sensors for information systems."[13]***

This definition accurately encompasses all aspects of the IoT – from the Dropcam, to the FitBit, to the Nest, to the smart phone. Likewise, it would also capture RFID chips and UPC codes that are scanned electronically.[14]

4. Are there ways to divide or classify the IoT landscape to improve the precision with which public policy issues are discussed?

Rather than subdividing the IoT landscape, we should instead do as we have done with all data, look to use not mode of collection. At the same time, we suggest that if the NTIA does a harms based analysis of IoT, the analysis should balance actual harms with concrete benefits.

Looking to use not collection

Regarding IoT, we agree with FTC Commissioner Ohlhausen that rather than focusing on limitations on collection, which can unintentionally burden development and innovation, we should focus on the way that data is used.

> I believe that it is important to seek an approach that protects consumers from substantial privacy harms while not hampering the economic and societal benefits that data-driven technology may offer. In pursuit of this goal, some have suggested focusing on the use of personal information and the impact on the individual, rather than attempting to safeguard privacy primarily by controlling information collection. Such use-focused approaches emphasize the difficulty of specifying unforeseen but valuable subsequent uses of data.[15]

We also agree with Commissioner Ohlhausen, that when data is collected, regardless of the medium, there should be:

- a framework that emphasizes preventing harmful uses of personal information,
- accountability for use of personal data however collected,
- a respect for context, and
- transparency about the use of such data with a concomitant ability of consumers to know if data has been used to disadvantage them.[16]

Fortunately, we have already established these mechanisms. When data is collected, regardless of the devices or format, privacy policies and terms of use provide consumers with the information regarding

---

[13] Kevin Ashton, POLITICO, *America last?*, *available at* http://www.politico.com/agenda/story/2015/06/kevin-ashton-internet-of-things-in-the-us-000102 (May 2015)

[14] This type of use was part of the origin of the term IoT. Kevin Ashton, *That 'Internet of Things' Thing RFID Journal*, (May 2009) *available at* http://www.rfidjournal.com/articles/view?4986

[15] *Re: Comments of Maureen K. Ohlhausen, Commissioner, Federal Trade Commission on Big Data, Consumer Privacy, and the Consumer Bill of Rights* at p 8 (Aug. 4, 2014)

[16] *Id.* at 9

how that data is used. Moreover, businesses are adapting consumer notices to provide them in context and more understandable terms.

If data is used in a manner materially different from the terms under which it was collected, the FTC has made clear that such alternative uses require prior affirmative consent[17] and could likely use it's Section 5 authority to bring action against such non-consensual different use.

Analysis should Balance Real World Harms

> *The injury must not be outweighed by any offsetting consumer or competitive benefits that the sales practice also produces.*
>
> -- FTC Policy Statement on Unfairness, Dec. 17, 1980[18]

When looking at possible "harms" from IoT, we suggest the NTIA look to the FTC policy statement on unfairness which sets out the guidelines for how to balance real world harms:

> Most business practices entail a mixture of economic and other costs and benefits for purchasers. A seller's failure to present complex technical data on his product may lessen a consumer's ability to choose, for example, but may also reduce the initial price he must pay for the article. The Commission is aware of these tradeoffs and will not find that a practice unfairly injures consumers unless it is injurious in its net effects. The Commission also takes account of the various costs that a remedy would entail. These include not only the costs to the parties directly before the agency, but also the burdens on society in general in the form of increased paperwork, increased regulatory burdens on the flow of information, reduced incentives to innovation and capital formation, and similar matters.[19]

So if the NTIA decides to investigate potential "harms" of IoT, it should do so only after balancing actual harms, if any, against actual real world beneficial uses of IoT.

15. WHAT ARE THE MAIN POLICY ISSUES THAT AFFECT OR ARE AFFECTED BY IOT? HOW SHOULD THE GOVERNMENT ADDRESS OR RESPOND TO THESE ISSUES?

As stated above, if the NTIA or any government agency chooses to begin looking into potential policy issues regarding privacy of IoT, it should be done by balancing real world harms with real world benefits. This avoids regulating against fictitious problems and instead allows growth and development of IoT.

16. HOW SHOULD THE GOVERNMENT ADDRESS OR RESPOND TO CYBERSECURITY CONCERNS ABOUT IOT?

Because the same cybersecurity concerns exist for IoT as for any internet accessible device, we suggest that the NTIA and the FTC engage in greater efforts to educate consumers and businesses about security protections.

---

[17] *See, e.g.*, *Letter From Jessica Rich, Director, Bureau of Consumer Protection, To Bankruptcy Court Expressing Bureau Concerns About the Possible Sale by RadioShack of Certain Consumer Personal Information As Part of the Bankruptcy Proceeding* at p 5 (May 18, 2015) ("As in *Toysmart*, our concerns about the transfer of customer information inconsistent with privacy promises would be greatly diminished if the following conditions were met … The buyer agrees to obtain affirmative consent from consumers for any material changes to the policy that affect information collected under the RadioShack policies.")

[18] FTC Policy Statement on Unfairness, Dec. 17, 1980, *available at* http://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness

[19] Transcript of FTC Workshop "*Big Data: A Tool For Inclusion Or Exclusion*," Sept. 14, 2014 reported by Jennifer Metcalf p. 155

16 A. What are the cybersecurity concerns raised specifically by IoT? How are they different from other cybersecurity concerns?

We find that the cybersecurity concerns for IoT are substantially the same for any device that accesses the internet.

16 C. What role or actions should the Department of Commerce and, more generally, the federal government take regarding policies, rules, and/or standards with regards to IoT cybersecurity, if any?

We suggest that the NTIA and FTC avoid establishing additional cyber security policies, rules, and/or standards because they would be either duplicative or conflicting with existing guidelines regarding cybersecurity for devices connecting to the internet.

Instead we suggest that the NTIA and FTC mount a campaign to educate consumers and businesses about how to better secure their devices that connect to the internet. This could include talks about engaging in end-to-end security, looking for SSL, and proper generation, use, and storage of passwords.

17. How should the government address or respond to privacy concerns about IoT?

The government should apply its existing enforcement tools regardless of how the data is collected. If the concern then pivots to use, we suggest that the government engage in balanced evidence-based research before taking steps to govern or regulate IoT.

We recommend this analysis adopt the following 3-step approach based on the FTC's unfairness doctrine:[20]

1. Search for actual harms: Look to see if consumer complaints point to real-world (not theoretical) harms which exist from the use and growth of big data. Such analysis should separate out actual harms from general privacy anxiety.[21]
2. Balance harms: If harms exist, they must be balanced against the actual benefits of big data (some of which are discussed within these comments). This balancing should include down-stream impact of limitations on the use or collection of big data.
3. Analyze existing laws. To avoid overly restrictive new laws, there should be research of existing laws that mitigate identified harms not offset by benefits.

Moreover, talking in hypotheticals often leads to a conversation of what may be and not what is so. This prevents a discourse of actual harms and instead leads to a "parade of horribles." Any discussion of privacy concerns about IoT should avoid the words "may", "might" and "could" as it does not describe what is.

Role for Government

The role for government should be in areas where users and business cannot act alone, including law enforcement, international data flows, and pre-empting a patchwork of state laws conflicting with

---

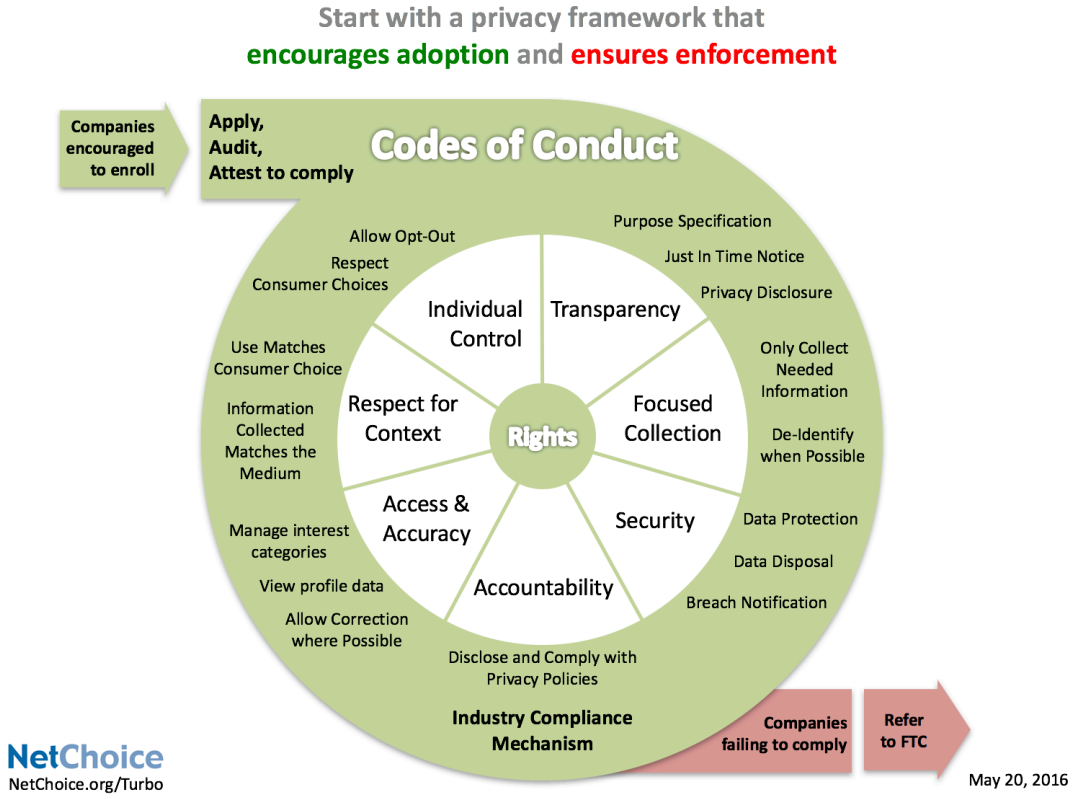
[20] FTC Policy Statement on Unfairness, Dec. 17, 1980, *available at* http://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness

[21] The greatest number of FTC complaints are about advertising related to mobile plans, rates or coverage areas; unsolicited mobile text messages; problems with mobile applications or downloads; other mobile device problems; charges for calls to "toll-free" numbers; unauthorized charges, such as charges for calls consumers did not make; unauthorized switching of consumers' phone service provider; misleading pre-paid phone card offers; as well as complaints about VoIP services; unsolicited faxes; etc. (Fraud Category). FTC, Sentinel CY 2014, at 79 (2015), available at https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2014/sentinel-cy2014-1.pdf.

federal interests. Government should use its powers to pursue online fraud and criminal misuse of data, not to create rules that narrowly prescribe what and how data should be used.

Overall, we support the notion that companies and customers – not governments – must take the lead on data privacy. Companies need to pursue innovation without asking for permission from government agencies. And consumers must understand the decisions they make, but they must be allowed to make those decisions.

We offer this conceptual view of an industry self-regulatory framework that dynamically adapts to new technologies and services, encourages participation, and enhances compliance.



As seen in the conceptual overview, components of the Privacy Bill of Rights form the aspirational core that influences business conduct regarding data privacy. From previous work by the FTC, NAI, and IAB, we've established the foundational principles for the collection and use of personal information: individual control, transparency, respect for context, access and accuracy, focused collection, accountability, and security.

Participating companies would publicly attest to implement Codes within their business operations, including periodic compliance reviews. If a company failed to comply with the adopted Codes, the FTC and state Attorneys General could bring enforcement actions, as is currently the case when companies fail to honor their adopted privacy policies.

Significantly, this framework does not require additional legislation to establish any new laws regarding IoT or similar data uses.

19. In what ways could IoT affect and be affected by questions of economic equity?

Because the issues surrounding IoT are the same surrounding any device that has historically connected to the internet, we find it unnecessary to revisit this issue as the FTC recently issued a white paper[22] on this.

However, should the NTIA seek to look into issues of "economic equity" it should look at real world examples of ways that IoT has decreased economic inequality. For example, IoT can help overcome the digital divide and bring medical assistance to those who otherwise would not have it. At the same time, NTIA should follow FTC unfairness doctrine and avoid looking at theoretical harms -- limiting analysis to actual harms if they exist.

IoT can help overcome the digital divide and bring medical assistance to those who otherwise would not have it.

24. What factors can impede the growth of the IoT outside the U. S. (*e.g.,* data or service localization requirements or other barriers to trade), or otherwise constrain the ability of U.S. companies to provide those services on a global basis? How can the government help to alleviate these factors?

As stated above, IoT does not require changing the internet – a system of locally connected networks. This makes sense. Consider a local network – e.g. a consumer's home network. Installation of a Nest thermostat does not require the consumer to fundamentally change the network.

Some have raised concerns about creating enough IP addresses to cover all the new devices (i.e. running out of IP addresses).[23] Fortunately, engineers and innovators have already addressed this concern with the introduction of IPv6.[24]

However, as IP addresses are connected to devices not places, the existing expectation of IP localization is lost. Today, IP addresses mostly operate similar to area codes. But much like how the cellphone disconnected area codes from regions of the country, IP addresses will soon no longer be tied to segments of the world. This will require routers to increase their searches for proper IP addresses as they route traffic to greater unknown locations. The result will likely require routers to increase in RAM, CPU speeds, and cooling capabilities.

These new burdens on routers from the dissociation of IPs from regions is an area ripe for NTIA analysis.

We thank you for your consideration and we look forward to working with the NTIA to enhance the growth of IoT.

Sincerely,

Carl Szabo
Senior Policy Counsel, NetChoice

NetChoice is trade association of leading e-commerce and online businesses. *www.NetChoice.org*

---

[22] FTC Staff Report, *Internet of Things - Privacy & Security in a Connected World* (Jan. 2015)

[23] Michael Ansaldo, *Running out of Internet addresses: What IPv4 exhaustion means for you*, TechHive (Nov. 2015), *avialble at* http://www.techhive.com/article/3007054/home-networking/running-out-of-internet-addresses-what-ipv4-exhaustion-means-for-you.html.

[24] *See e.g.*, New Jersey Institute of Technology, *We Need Engineers Ensuring The Web Doesn't Run Out Of Addresses*, *available at* http://graduatedegrees.online.njit.edu/msee-resources/msee-infographics/we-need-engineers-ensuring-the-web-doesnt-run-out-of-addresses/.