



June 1, 2016

Via email [iotrfc2016@ntia.doc.gov](mailto:iotrfc2016@ntia.doc.gov)

Mr. Lawrence Strickling  
Assistant Secretary of Communication and Information  
National Telecommunications and Information Administration  
U.S. Department of Commerce  
1401 Constitution Avenue NW.  
Room 4725  
Attn: IOT RFC 2016  
Washington, DC 20230

Re: Request for Comments on the Benefits, Challenges, and Potential Roles for the Government in  
Fostering the Advancement of the Internet of Things  
Docket Number: 160331306-6306-01

Dear Mr. Strickling,

In response to the request for comments, the Online Trust Alliance (OTA), hereby provides this response. As a 501(c)(3) non-profit, OTA's mission is to enhance online trust and empower users while promoting innovation and the vitality of the Internet. OTA works to educate businesses and policy makers, to drive adoption of responsible privacy practices and security standards to promote commerce and enhance the security of our nation's critical infrastructure. OTA prides itself as an active and objective participant in multi-stakeholder initiatives including fighting spam and botnets, and promoting Internet governance, mobile security, and privacy best practices.<sup>1 2</sup>

OTA remains concerned about the long-term negative impact to consumer trust and confidence related to online services. Collectively the public and private sectors must move beyond a compliance mindset to becoming data stewards while respecting consumer choices and privacy. Unfortunately in all too many cases, in the rush to market, companies have disregarded these efforts resulting in a growing level of mistrust. As experienced with consumer's response and use of ad blocking technologies, we are experiencing chilling disruptive effects to ad supported online services. Long-term they risk hampering of the free exchange of ideas, and disproportional disenfranchising of vulnerable segments of society.

---

<sup>1</sup> OTA Anti-Botnet Initiative <https://otalliance.org/resources/botnets>

<sup>2</sup> OTA Convenes Internet Governance Leaders to Address Risks of gTLDs <https://otalliance.org/news-events/press-releases/internet-governance-leaders-convene-discuss-domain-collisions>

In considering many of the questions raised in the RFC, it is important to note the OTA convened and established a multi-stakeholder working group nearly 16 months ago to. This working group today includes nearly 100 participants from both the private and public sectors addressing the security, privacy and long-term sustainability issues and risks. This effort has successfully addressed many of the policy issues raised in this RFC.

Earlier this year the OTA released the IoT Trust Framework, including 30 critical controls and criteria which serve as the foundation for a self-regulatory and certification program (See exhibit A). Today, this Framework is being embraced by a wide range of organizations providing prescriptive and actionable advice for developers and service providers. The success of the working group has been due in part to our ability to leverage learnings from past NTIA multi-stakeholder efforts, the standards community and others working groups, assuring balance and objectivity, without be dominated by special interest groups, trade organizations or any single constituency. Bi-weekly meetings continue today, with draft documents and resources posted frequently reflecting working group input and soliciting input from the public. Information and resources are posted at <https://otalliance.org/loT>.

The following comments are submitted in response, referencing the question and numbering in the RFC;

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? What are the most significant new opportunities and/or benefits created by IoT, be they technological, policy, or economic?

IoT presents significant challenges for both the public and private sectors. With the rapid introduction of these products, the challenges in IoT are unlike those observed with previous technologies. This is in part due to the broad range, sheer number and interconnectivity and dependence of devices. IoT in itself is becoming a disruptive force, impacting nearly every facet of our lives and economy. Today IoT solutions span from connected cars, homes and industrial controls, to medical devices and wearable technologies. Not unlike the dot-com bubble, in this rapid race to market we are witnessing a lack of adherence to security basics and responsible privacy practices. Similarly, we are now starting to witness market consolidation and attrition, raising issues about the security of the installed base of orphaned devices.

The rush to market brings reliance on and usage of off-the-shelf components and software libraries, common in the device supply chain. Without the ability to complete security risk assessments and track potential vulnerabilities, all devices downstream could be impacted. We will see a spiraling increase in the number of vulnerable IoT implementations creating growing unaddressed risks.

Of particular concern is the amount of discreet and “ambient” data which is being collected by an increasing number of devices and manufacturers. In general, there is a lack of disclosure about these practices prior to product purchase which are required for product functionality. Little is disclosed on how personal or usage data is collected, shared, or retained. Unlike visiting a web site or downloading a mobile app, IoT products may be costly or difficult for a consumer to abandon should they find the data policies unacceptable. Data collection notices need to be presented in a concise format, including disclosure of any product features dependent on any personal data collection, prior to consumer purchase of the product or service. Unfortunately many of the existing disclosures are failing to be made, raising several significant policy and legal issues. Additionally, as such

products are typically dependent on a mobile and cloud service, the long-term supportability beyond the traditional product warranty period also needs to be disclosed.

The recent experience with Alphabet's Nest shutting down support for purchasers of Revolv home hubs, rendering users' \$300 devices useless, "bricking" them, illustrates the problem. Fortunately Nest has offered users device refunds. In the absence of policies and norms, such practices threatened to stifle consumer purchases and IoT growth. (See IoT framework #17).

3. With respect to current or planned laws, regulations, and/or policies that apply to IoT: Are there examples that, in your view, foster IoT development and deployment, while also providing an appropriate level of protection to workers, consumers, patients, and/or other users of IoT technologies?

In the absence of industry norms and regulatory landscape, innovation in many way is being stifled, because developers are at a loss about what are acceptable practices. With the lack of prescriptive guidance from key government agencies, developers are left to their own accord. This was a driving force for industry to join together and develop the IoT Trust Framework. We believe such a framework, leading to an enforceable code of conduct, provides developers and regulators clear direction while recognizing that there is no absolute security and privacy, and also acknowledging that yesterday's standards may no longer be sufficient or appropriate.

4. Are there ways to divide or classify the IoT landscape to improve the precision with which public policy issues are discussed? If so, what are they, and what are the benefits or limitations of using such classifications? Examples of possible classifications of IoT could include: consumer vs. industrial; public vs. private; device-to-device vs. human interfacing.

IoT has many distinct designs and functions including one-way sensors and devices, integrated systems that interact with other users and other systems, machine-to-machine interactions, etc. Additionally, such terms and elements vary by different business sectors and their respective norms and regulatory frameworks. Given the wide variety, it is important to segment devices and categories across the IoT landscape. The IoT working group, for example, elected to focus on connected home and consumer wearable technologies, omitting medical devices and the connected car because these are regulated by other industry and policy bodies. In addressing IoT, suggested classifications include: 1) industrial controls and sensors; 2) connected automobiles, 3) medical devices, 4) wearable technologies (including fitness related devices), and 5) smart home / connected devices. Such a matrix should consider active and passive systems.

5. Please provide information on any current (or concluded) initiatives or research of significance that have examined or made important strides in understanding the IoT policy landscape. Why do you find this work to be significant?

The IoT Trust Framework is a leading worldwide example of an open and inclusive initiative resulting in a framework based on recent research and fact-based use case scenarios. Unique to this effort has been the level of international input and ability to measure adoption and assertions as part of a self-regulatory framework. Supporting the framework, OTA has published a draft resource guide including use-case scenarios, references and resources.<sup>3</sup>

---

<sup>3</sup> IoT Trust Framework Resource Guide <https://otalliance.org/initiatives/internet-things>

6. What technological issues may hinder the development of IoT, if any? What can the government do, if anything, to help mitigate these technical issues? Where may government/private sector partnership be beneficial?

The OTA believes the adoption of a comprehensive self-regulatory framework should be encouraged through incentives and removal of barriers to adoption. Such incentives might include a “safe harbor” type program and / or protection from law suits. In addition, grants should be developed to further drive the awareness and adoption of these best practices and certification programs, while publishing prescriptive guidance and resources.

7. NIST and NTIA are actively working to develop and understand many of the technical underpinnings for IoT technologies and their applications. What factors should the Department of Commerce and, more generally, the federal government consider when prioritizing their technical activities with regard to IoT and its applications, and why?

The common threat impacting infrastructure and network security (along with users’ personal safety) associated with IoT devices, is the issue of lifecycle and sustainability. Having clear guidance and requirements for support and patching, processes for vulnerability notification (Principle #5), along with control of data retention are areas where little attention is being paid today. Left unchecked, significant concerns include that devices may be orphaned or abandoned by manufactures, ceasing patches for known vulnerabilities, or users may transfer devices without the ability to review security updates or notices. The lack of current emphasis on sustaining IoT security over time is problematic. Further, consumer information on support time frames is limited or non-existent. Similarities in other industries should be considered such as the requirement of automotive manufacturers to provide safety recalls for a set number of years, independent of the vehicle warranty, where the manufacturer is obligated to provide a free remedy.

8. How will IoT place demands on existing infrastructure architectures, business models, or stability?

In terms of business models, one important area emerging in IoT innovation is deployment of the data-driven business model where consumers may pay low or no out-of-pocket costs for the device or service, but instead “pay” via a company’s collection of users’ data and reuse of such data as a revenue stream. Already established in online games, apps, etc., the rising use of IoT data as a revenue model raises important concerns regarding privacy, data ownership, and potential exploitation of or bias against users via their data.

A second concern is the impact of devices on home networks, where a vulnerable or rogue device or application can impact not only the home network, but equally as important, impact the ISP or carrier providing connectivity. While ISPs may see malicious traffic come from a home IP address, they do not have a line of sight into the specific devices. If ISPs attempt to cut off or limit connectivity to a compromised device, the impact to the home systems can be significant such as disabling security systems, access controls and other integrated systems. In the past, some ISPs have placed compromised homes in a “walled garden” limiting access to security resources. It is unknown the impact such an approach would have on the home network and integrated services which consumer may rely on for basic and necessary home needs.

9. Are there ways to prepare for or minimize IoT disruptions in these infrastructures? How are these infrastructures planning and evolving to meet the demands of IoT?

The component supply chain and use of open source software code introduces inherent security risks. As experienced in the PC clone market a decade ago and in some early mobile app development re-using public code libraries, IoT introduces downstream security and compatibility issues. Recognizing such risks, minimal testing and certification of components is encouraged including the requirement for developers to inventory use of such code and mechanisms to alert them on security risks.

10. What role might the government play in bolstering and protecting the availability and resiliency of these infrastructures to support IoT?

OTA proposes NTIA and government consider providing incentives to companies to be certified for compliance to baseline criteria and self-regulatory frameworks. Such incentives could range from protection against class action suits to positive recognition. Possible models could include a certification seal program based on core criteria (such as the IoT Trust Framework) not unlike the Energy Star program recognizing energy efficient products. Additionally, if USG were to set minimal standards for its use of IoT it could help drive standards in the private sector.

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 noted in number 8, the rise in IoT of data collection as a revenue stream has important policy implications. The challenges include specific questions of personal privacy and data ownership, but also span risks for data profiling and discriminatory application of data analysis (for example, using health tracker activity data in assessing a person's job capabilities, etc.), as well as potential inequalities in access due to the relative 'value' of a user's data. Further, the enduring nature of digital data raises concerns about consumers' ability to remove / correct historical data. Policy responses to these topics should include evaluation of similar issues and solutions such as those surrounding consumers' ability to challenge and correct their credit report data.

16. How should the government address or respond to cybersecurity concerns about IoT? What are the cybersecurity concerns raised specifically by IoT? How are they different from other cybersecurity concerns? How do these concerns change based on the categorization of IoT applications (e.g., based on categories for Question 4, or consumer vs. industrial)? 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?

The IoT ecosystem is unique in that typical solutions encompassed three-dimensions each of which are dynamic requiring concurrent security assessments. These include 1) the physical device or sensors, 2) the supporting web or mobile application(s) and 3) the back-end cloud service supporting the device and applications. The layers and flow of data increase the risk footprint. All of which must be addressed both concurrently and on an ongoing basis. As outlined, the best role for the federal government is to fund data exchanges (such as the creation of an IoT ISAC), training resources and multi-stakeholder efforts and workshops. Adding to the security risk is the lack of adequate credential authorization and need to move to a multi-factor or federated password systems. With the exponential increase in the number of unique devices within a home, it is inevitable that users will reuse simple passwords, increasing the risk of device and systems takeover, resulting not only in malicious activities and compromise of personal privacy, but increasing the risk of personal harm, theft and damages.

17. How should the government address or respond to privacy concerns about IoT? (see question 16)

As addressed in previous questions, the amount of data being collected, and the added data attributes (location, personal lifestyle), present benefits but at the same time raise significant risks and issues. Device terms of use and privacy policies in general should not require that a user opt-in to sharing of their personal information in order to use the primary device features and benefits. In addition, IoT presents both form factor challenges and time of disclosures challenges regarding consumer understanding of the data practices. For example, a user should not learn *after* installing a 60" TV that some of the core features of the product are dependent on sharing of their personal viewing habits with third parties. Not unlike product packaging stating "batteries required", if such data sharing is required, product packaging should disclose it and state what, if any, product features require this collecting and sharing of user data. Conversely, anonymous data and device telemetry limited to product support, service and product improvement should be considered acceptable use and not require a user to opt-in, so long as an opt-out capability is provided.

Ideally the use of a standard privacy disclosure notice not unlike the FCC Labels for Broadband Services or required by the FDIC privacy policies should be considered. Such standardized notices allow consumers the ability to compare practices so they can make informed choices about available broadband services and banking options.

18. Are there other consumer protection issues that are raised specifically by IoT? If so, what are they and how should the government respond to the concerns?

With the sheer number of devices being installed and used, the ability to collect and capture a consumer's digital life in detail is significant, including biometric data. When appended with other sources of big data and data analytics, the value for marketers and their ability to monetize this data is significant. Unlike a user visiting a consumer-facing website where the content is funded by advertising (both general and interest-based), a consumer purchasing an IoT device should not by default be required to "pay" for the device in perpetuity by sharing their and their family's personal data. In general any such data collection and sharing should require a user to opt in and should not limit device core functionality.

Recently, manufacturers and carriers have looked to introduced two-tier pricing or models where products can be subsidized by the collection and sharing of user's personal data. Such practices have the risk of creating a "privacy divide" based on income levels and should require added disclosures as they may inadvertently disproportionately impacting disadvantaged communities or groups. In addition the security and privacy implication of IoT may lead to personal and physical safety risks.

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

As noted in questions 15 and 18, a potential impact of IoT on economic equality is the arena of personal data. In terms of data use / reuse and ownership concerns include profiling and misuse along with consumers ability to correct harmful errors. In terms of using data sharing as a potential element of revenue or price setting, the concerns include tiered pricing which could make privacy a sort of 'luxury good' only those with enough income can afford. Additionally, IoT devices need to address core accessibility requirements, maximizing usage for users of all ages and functional and cognitive capabilities.

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?

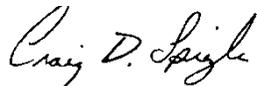
Privacy Shield and international data breach legislation increasing will have an impact on the data collection and privacy practices for every IoT device. Developers and manufactures should design their products and services with this in mind. USG can best help by embracing the opt-in and data collection and sharing requirements being mandated beyond our borders.

25. Are there IoT policy areas that could be appropriate for multi-stakeholder engagement, similar to the NTIA-run processes on privacy and cybersecurity?

Based on success to-date, OTA discourages standing up a new multi-stakeholder initiative. The OTA and the IoT working group believe that NTIA launching a new initiative risks creating confusion and stalling the adoption of generally accepted best practices. Rather than risk “reinventing the wheel,” a better use of resources would be to aid in driving adoption, and provide funding and incentives to support established initiatives, including the funding of pilot programs not unlike those created by the NSTIC program.

In summary, OTA looks forward to working with NTIA on this and related efforts to enhance consumers’ control of their data, while promoting innovation, resiliency in our critical infrastructure, economic growth and an open internet. Collectively through an open multi-stakeholder process we have already accomplished a great deal. With the support and participation of NTIA on this industry-convened initiative we can take IoT security and privacy to the next level, while promoting innovation, trust and economic growth.

Sincerely,



Craig D. Spiegle  
Executive Director and President  
Online Trust Alliance  
[Craigs@otalliance.org](mailto:Craigs@otalliance.org)  
<https://otalliance.org>  
+1 425-455-7400

Cc: Mr. Travis Hall, NTIA

## OTA IoT Trust Framework – Released 3/2/2016

IoT Trust Framework ● Required ○ Recommended N/A – Not Applicable	Connected Home	Wearable Tech
<b>SECURITY</b>		
1. Ensure devices support current generally accepted security transmission protocols. All personally identifiable data in transit and in storage must be encrypted using current generally accepted security standards. This is including but not limited to wired, WI-FI and Bluetooth connections.	●	●
2. Authentication credentials, including but not limited to passwords shall be salted, hashed and/or encrypted.	●	●
3. All IoT support web sites must fully encrypt the user session. Current best practices include HTTPS or HTTP Strict Transport Security (HSTS) by default, also known as AOSSL or Always On SSL.	●	●
4. IoT support sites must implement regular monitoring and continual improvement of site security and server configurations to acceptably reduce the impact of vulnerabilities. Perform penetration tests at least annually.	●	●
5. Establish and maintain processes and systems to receive, track and promptly respond to external vulnerabilities reports from third parties including the research community. Remediate post product release design vulnerabilities and threats in a publically responsible manner either through remote updates and/or through actionable consumer notifications, or other effective mechanism(s).	●	●
6. All software and/or firmware updates, patches and revisions must either be signed and/or otherwise verified as coming from a trusted source. Updates and patches should not modify user-configured preferences, security and/or privacy settings without user notification.	●	●
7. Ensure all IoT devices and associated software, have been subjected to a rigorous, standardized software development lifecycle process including unit, system, acceptance, regression testing and threat modeling, along with maintaining an inventory of the source for any third party/open source code and/or components utilized. Employ generally accepted code and system hardening techniques.	●	●
8. End-user communications including but not limited to email and SMS, must adopt authentication protocols to help prevent spear phishing and spoofing. For example for email communications must adopt SPF, DKIM and DMARC, for all security and privacy related communications and notices.	●	●
9. For email communications within 180 days of publishing a DMARC policy, implement a reject policy, helping ISPs and receiving networks to reject email which fail email authentication verification checks.	○	○
10. IoT vendors using email communication must adopt transport-level confidentiality including generally accepted security techniques to aid in securing communications and enhancing the privacy and integrity of the message.	○	○

IoT Trust Framework ● Required ○ Recommended N/A – Not Applicable	Connected Home	Wearable Tech
<b>USER ACCESS &amp; CREDENTIALS</b>		
11. For user access, provide unique system generated or single use passwords; or alternatively use secure certificate credentials. As necessary, require use of unique passwords for administrative access, delineating between devices and services and the respective impact of factory resets.	●	●
12. Provide generally accepted recovery mechanisms for IoT application and support passwords and/or mechanisms for credential re-set using multi-factor verification (email and phone, etc.) where no user password exists.	●	●
13. Companies must take steps to protect against ‘brute force’ and/or other abusive login attempts (such as automated login bots, etc.) by locking or disabling user and device support account(s) after a reasonable number of invalid log in attempts.	●	●
14. Provide users notification of password reset or change utilizing secure authentication and /or out-of-band notice(s).	●	●
15. Enact a breach response and consumer notification plan to be reevaluated, tested and updated at least annually or after significant internal system, technical and / or operational changes.	●	●
<b>PRIVACY, DISCLOSURES &amp; TRANSPARENCY</b>		
16. Ensure privacy, security and support policies are easily discoverable, clear and readily available for review <u>prior</u> to purchase, activation, download or enrollment. In addition to prominent placement on their website, it is recommended companies utilize QR Codes, user friendly short URLs and other similar methods.	●	●
17. Disclose the duration of security and patch support, (beyond product warranty). Such disclosures should be aligned the expected lifespan of the device.	●	●
18. Conspicuously disclose what personally identifiable and sensitive data types and attributes are collected and how they are used, limiting collection to data which is reasonably useful for the functionality and purpose for which it is being collected. Disclose and provide consumer opt-in for any other purposes.	●	●
19. Disclose what features will fail to function if connectivity becomes disabled or stopped including but not limited to the potential impact to physical security.	●	●
20. Disclose the data retention policy and duration of personally identifiable information.	●	●
21. IoT devices must provide notice and/or request a user confirmation when initially pairing, onboarding and/or connecting with other devices, platforms or services.	●	●

22. Publically disclose if and how IoT device/product/service ownership may be transferred (e.g., a connected home being sold to a new owner or sale of a fitness tracker).	●	●
23. Only share consumers' personal data with third parties with consumers' affirmative consent, unless required and limited for the use of product features or service operation. Require third party service providers are held to the same polices including holding such data in confidence and notification requirements of any data loss/breach incident and/or unauthorized access	●	●
24. Provide controls and/or documentation enabling the consumer to review and edit privacy preferences of the IoT device including the ability to reset to the "factory default."	●	●
25. Commit to not sell or transfer any identifiable consumer data unless it is a dependent part of the sale or liquidation of the core business which originally collected the data, providing the acquiring party's privacy policy does not materially change the terms. Otherwise notice and consent must be obtained.	●	●
26. Provide the ability for a consumer to return a product without charge after reviewing the privacy practices that are presented prior to operation, provided that such terms are not conspicuously disclosed prior to purchase. The term (number of days) for product returns shall be consistent with current exchange policies of the retailer, or specified in advance.	●	●
27. Whenever the opportunity is presented to decline or opt out of any policy, the consequences must be clearly and objectively explained, including any impact to product features or functionality. It is recommended the end-user value of opting in and/or sharing data be communicated to the end-user.	●	●
28. Publically post the history of material privacy notice changes for a minimum of two years.	○	○
29. Provide the ability for the user or proxy to delete, or make anonymous personal or sensitive data stored on company servers (other than purchase transaction history) upon discontinuing, loss or sale of device.	○	○
30. Provide device or service data erasure and zeroization in the event of loss or sale.	○	○

### Terminology, Definitions & Clarifications

1. Unless specified otherwise, the terms device manufacturers, vendors, application developers, service providers and platform operators are all indicated by the term "Companies." The inclusion of platforms is paramount as the IoT may be headed to a future where platform and OS providers and their respective connected ecosystems communicating on a seamless network may pose security and privacy risks.
2. It is expected that companies, products and services are in compliance with any law or regulation of the jurisdiction that governs the collection and handling of personal and sensitive information. Failure to do so constitutes non-compliance with this framework and results in automatic disqualification from any forthcoming code of conduct or certification program.
3. It is expected companies disclose details of sharing data with law enforcement and reference any applicable transparency reports as legally permitted.
4. Smart devices refer to devices (and sensors) which are networked and may only have one-way communications.
5. Medical devices regulated by the FDA are beyond the scope of the Framework, yet the majority of the criteria are deemed to be applicable.