Online Trust Alliance

March 13, 2017

Via email iotrfc2017@ntia.doc.gov

Mr. Travis Hall
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW. /Room 4725
Attn: IOT RFC 2017
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 Green Paper
Docket Number: 170105023-7023-01

Dear Mr. Hall,

The Online Trust Alliance (OTA), hereby provides this response to the RFC and thanks the Department of Commerce (DOC) for their leadership and efforts to help address the mounting security and privacy risks associated with the rapid rise in the use of Internet of Things (IoT) devices. For background OTA is a 501(c)(3) non-profit with the mission is to enhance online trust and empower users while promoting innovation and the vitality of the Internet.

Society and the global economy are witnessing an unparalleled level of innovation being brought forth from the introduction of thousands of new IoT devices. While it is important to recognize there is no perfect security or privacy, all too many IoT devices appear to be designed primarily for convenience and functionality. Long-term security or "sustainability" of the devices and the control and privacy of the associated data is conspicuously absent. Many of these "smart" devices are often not as smart as suggested.

Much like global warming or industrial pollution, there will be long-term consequences resulting from inaction with IoT threats. The impact of these threats have jumped to the physical world, ranging from unlocking doors, turning on cameras, shutting down critical systems and theft of personal property. The lack of action by industry has created a treasure chest ripe for abuse by white collar criminals, terrorists and state sponsored actors as IoT devices become weaponized. As recently reported, the US Central Intelligence Agency (CIA) has been exploiting these vulnerabilities and we should also expect other intelligence gathering organizations and criminals to be doing the same.[1] Left unchecked we may realize a "digital environmental disaster".

[1] CIA Hacking of IoT Devices https://www.wsj.com/articles/wikileaks-posts-thousands-of-purported-cia-cyberhacking-documents-1488905823 (WSJ March 7, 2017)

Foreseeing these concerns, in mid-2014 OTA convened and established a multi-stakeholder working group. This working group has included nearly 100 participants addressing the IoT security, privacy and long-term sustainability risks. Focusing on consumer grade devices, the OTA released version 2.0 IoT Trust Framework (Framework) in January 2017, (Exhibit A). The Framework has since been endorsed by international collation of stakeholders.[2] The Framework's principles serve as a guide to developers and as a risk assessment guide for the public and private sector. OTA asserts that companies who can demonstrate they have fully adopted the Framework should be afforded "safe-harbor' from regulators as well as protection and defense from product liability lawsuits.

A Collaborate and Shared Responsibility

The DOC has an important role to promote such efforts. Unfortunately to-date multiple U.S. Government agencies are fragmenting the industry by asserting conflicting and overlapping roles and principles. Rather then re-invent the wheel, we recommend the DOC work cross both US Agencies as well as other international efforts and drive reconciliation of efforts. Doing so will provide significant benefits, offering market certainty and help ensure society has the potential to reap the benefits and promise of IoT.

In early March the OTA released a white paper entitled IoT Security; *A Collaborative & Shared Responsibility*. The paper outlines the roles of key stakeholders required to realize the promise of IoT, (Exhibit B). The following is a brief outline;

1. **Retailers, Resellers & E-commerce Sites** – The retail channel may be the most influential party holding the keys to change. By establishing minimum security and privacy standards for the products they sell, industry will have to change their design and support practices. Not unlike retailers pledging to not source products made by child labor or those from unsustainable forests, they play a pivotal role in setting baseline requirements and have an opportunity to drive change and help to protect society at large.
2. **Developers & Manufacturers** – Manufacturers need to disclose their security support commitment to users prior to purchase. Not unlike food nutrition labels, they need to articulate their security and privacy policies. Such notices should be included on product packaging and point of sale materials to easily inform the consumer prior to purchase. As an incentive, companies that adopt sound security principles and responsible privacy practices should receive preferential treatment and placement from retailers and third party independent reviews such as those recently announced by Consumer Reports.[3]
3. **Brokers, Builders, Car Dealers & Realtors** – A smart home or connected auto are attractive selling points for every buyer or renter. Often listed as a feature, sellers should be required to disclose all such devices, disable their access, and provide new owners the ability to re-set them. At "closing," completion of a car rental or sale sellers should be required to turn in their physical and digital keys, and remove all personal data. Leading trade groups have taken steps to help address top privacy issues.[4] In an efforts to address

[2] Collation embraces OTA IoT Trust Framework https://otalliance.org/news-events/press-releases/ota-calls-iot-cyberattacks-%E2%80%9Cshot-across-bow%E2%80%9D (January 5, 2017)
[3] Consumer Reports http://www.consumerreports.org/privacy/consumer-reports-to-begin-evaluating-products-services-for-privacy-and-data-security/ (March 6, 2017)
[4] Auto Dealers Association www.AutomotivePrivacy.com and National Association of REALTORS https://www.nar.realtor/

these issue and assist consumers, OTA and the National Association of REALTORS released several checklists for buyers, renters and sellers of smart homes and apartments.[5]

4. **Internet Service Providers (ISPs) & Carriers** – Recent incidents of botnets taking control of IoT devices has become a shot across the bow as high-profile websites have been rendered inaccessible. Today in several countries including Australia and Germany, ISPs block botnets emanating from residential IP addresses. Compromised users are placed in "walled gardens," having limited online access to help protect society from harm. While many have recognized this as a best practice, U.S. ISPs and wireless carriers are not required to take action and the majority have been unwilling to commit to do so.[6] This reluctance can be appreciated as is important to recognize ISPs should not have to fully bear the burden or cost of fixing devices they do not manage or become the consumer's "help desk".
5. **Regulators & Policy Makers** – Regulators need to recognize there is no perfect security or privacy. To promote innovation and commerce they should encourage self-regulation while providing a "safe-harbor" to device manufacturers who can demonstrate they have adopted reasonable security and responsible privacy practices. Conversely, companies that fail should be "put on notice" that they may be exposed to oversight, fines and or class-action suits.
6. **Consumers** – Consumers must recognize the need to patch and ultimately replace insecure devices beyond their expected security life. Not unlike recycling or having car emissions checked, the benefit is for the greater good of society. When buying a connected device one should review the company's support commitment and privacy policy. If this information is not readily available or if their privacy practices are unacceptable, look for another product. Consumers should not have to risk having their personal information collected, sold and shared without consent.[7] At the same time, opting into such data collection while realizing added benefits may be a fair value-exchange.

The OTA has focused on answering the following questions outlined in Appendix B of the Green Paper.

Is our discussion of IoT presented in the Green Paper are there issues that we missed, or that we need to reconsider? The following is a summary where we believe the DOC should consider adding clarification and taking action;

a) **Scope** – In developing policy and recommendations it is important to recognize one size does not fit all. IoT is quickly becoming the "Internet of Everything". The Green Paper acknowledges there is no consensus or a formal definition for "IoT". We recommend the DOC drive a common framework and taxonomy to help ensure all stakeholders are speaking the same language. As a starting point we recommend the DOC embrace the consensus of both the OTA IoT working group and that of the NTIA IoT Security Upgradability and Patching working group which have focused on consumer grade devices used in the home and office including wearable (non-medical) devices.[8] When developing policy it is equally important to segment recommendations between non-durable vs durable products.

---

[5] OTA Smart home Resources https://otalliance.org/SmartHome
[6] FCC Anti-Botnet Code of Conduct for ISPs http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG7-Final-Report.pdf (February 2012)
[7] See IoT Smart Home and Smart Devices Checklists https://otalliance.org/SmartHome
[8] NTIA Multi-stakeholder Process; Internet of Things (IoT) Security Upgradability and Patching https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security

b) Global Perspective & Free Flow of Data Cross Borders – A free and open internet is the foundation of the digital economy and we recommend the DOC promote global, voluntary and industry-led standards, frameworks and best practices. While a significant amount of IoT related innovation is accruing in the US, it is foreseeable that these devices will ultimately be used in other geographies and collect personal and sensitive data. For IoT to achieve scale, data must be able to flow not only between IoT devices, but in many cases back to the cloud platform that hosts the network running those devices. It is recommended that the DOC needs to continue to work globally supporting an industry-led global marketplace that supports free flow of information. This role should highlight the importance of complying with international privacy and data protections norms and standards such as the EU General Data Protection Regulation (GDPR) and Privacy Shield programs.[9]

c) **Privacy** – OTA appreciates the DOC recognizing the importance of advancing baseline privacy legislation. Such legislation needs to be independent of the technology or application being employed, but put the interests of the user first. Numerous studies have cited that privacy is a significant and growing barrier to IoT adoption.[10] Conversely when consumers know their privacy is protected by robust laws, transparent disclosures, choice and controls, they will have greater confidence in acquiring new technologies and services. OTA believes modernizing privacy frameworks for IoT and embracing ensure strong privacy protections and a Privacy Bill of Rights should be prioritized in order to foster the advancement of IoT and economic growth.[11]

OTA believes this is an essential area where the DOC needs to place consumer protection and trust as a priority. The data being collected by IoT devices redefines personal data. When appended with geo-location, biometrics and real time voice and video, the privacy issues are amplified. As observed with multiple missteps of leading manufacturers, it is clear privacy is taking a backseat to profit taking.[12] Below is a summary of specific privacy principles outlined in the Framework which the DOC should embrace. All IoT devices should;

i. Ensure privacy, security, and support policies are easily discoverable and available for review prior to purchase, activation, download, or enrollment.
ii. 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.
iii. Disclose the data retention policy and duration of personally identifiable information stored.
iv. Publically disclose if and how IoT device/product/service ownership and the data may be transferred.
v. Only share consumers' personal data with third parties with consumers' consent, unless required and limited for the use of product features. Require service providers be held to the same polices.
vi. Provide controls and/or documentation enabling the consumer to review privacy preferences of the IoT device including the ability to reset to the "factory default."
vii. 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.
viii. Publicly post the history of material privacy notice changes for a minimum of two years.

[9] General Data Protection Regulation (GDPR) https://en.wikipedia.org/wiki/General_Data_Protection_Regulation
[10] PEW Research http://www.pymnts.com/news/2016/consumers-wary-on-iot-privacy/
[11] Privacy Bill of Rights https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf (February 2012).
[12] Vizio FTC Settlement https://www.ftc.gov/news-events/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it (February 2017)

d) **Device Transferability** – The DOC needs to expand focus on the transferability of devices including re-sale, rental and/or gifting and the related data stored on the device, application and/or back end cloud services. As outlined in the Framework, it is recommended devices provide consumers an easily discoverable method to reset a device and application to factory settings, providing the ability for erasure and zeroization in the event of transfer, loss or sale. Further third party agents such a realtors and car dealers should either purge all data and user access upon transfer, or remind customers of the need to do so. Such re-sets should preserve all software and firmware updates to maximize the security of such devices when transferred.

e) **Vulnerability Reporting** – The Green Paper is silent on the role and importance of coordinated vulnerability reporting as it applies to IoT. The OTA IoT Framework and NTIA Vulnerability working group[13] identified this as one of the core security principles as outlined below:

> *Principle # 4 - Establish coordinated vulnerability disclosure including processes and systems to receive, track and promptly respond to external vulnerabilities reports from third parties including but not limited to customers, consumers, academia and the research community. Remediate post product release design vulnerabilities and threats in a publicly responsible manner either through remote updates and/or through actionable consumer notifications, or other effective mechanism(s). Developers should consider "bug bounty" programs, and crowdsourcing methods to help identify vulnerabilities that companies' own internal security teams may not catch or identify.*

In response to this RFC, a collation including OTA has highlighted this recommendation and submitted a separate response.[14] It is recommended the DOC; a) Articulate the benefit of adopting coordinated vulnerability disclosure and handling processes and b) commit to continue working with stakeholders to promote coordinated voluntary adoption of vulnerability disclosure and handling processes.

Supporting this importance of this capability, as part of the annual Online Trust Audit, OTA provides sites bonus points for sites having an easily discoverable method to reporting bugs, site and/or application vulnerabilities.[15] Sites which include discoverable links to reporting forms or landings pages through a link on the footer of the home page or other mechanisms can realize maximum scoring.

f) **Voice Interfaces** – As more devices are enabled for voice controlled (Google Home and Amazon Echo), this voice activation has become an evolving threat and abuse vector. The DOC should explore these issues and work to promote best practices to address the risk of abuse. Not unlike forcing the use of unique passwords on install, ideally in the future voice activation platforms and devices will require the use of user authentication. This can range from the use of an "authorization password" or employ voice recognition signatures for key safety related functions.

---

[13] NTIA Multi-Stakeholder Vulnerability working group https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities

[14] RFC submission for vulnerability reporting http://otalliance.actonsoftware.com/acton/attachment/6361/f-00a3/1/-/-/-/-/NTIA%20RFC%20Green%20Paper%20-%20Vunerability%20.pdf

[15] OTA annual Online Trust Audit – 2017 methodology https://otalliance.org/TrustAudit.

What should the next steps be for the Department in fostering the advancement of IoT?

To drive innovation and efficiencies, industry needs a single voice for security and privacy best practices and standards voice among government agencies. DOC should become an advocate for other federal agencies to embrace similar principles. Doing so will benefit industry significantly including startups who do not have the resources to navigate the varied direction and messages being advanced. Such efforts can help to accelerate the introduction of safe and secure products to the market.

Second the DOC should engage with Congress in support of such efforts including the Developing Innovation and Growing the Internet of Things Act (DIGIT Act).[16] The Act as proposed would convene a working group of federal entities that will consult with private sector to provide recommendations to Congress. These recommendations would focus on how to plan for, and encourage, the growth of the IoT and ideally integrate security, privacy and sustainability principles. Third the DOC should track adoption of principles and provide early adopters positive and public affirmation. Such tracking is a key metrics to measure the effectiveness and impact of NTIA and the Internet Policy Task Force.

Conclusion

In summary, the OTA commends the DOC is their work to help address the benefits, risks and threats of IoT. Initial efforts of convening multi-stakeholder efforts are encouraging and an important step. 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 we can take IoT security and privacy to the next level, promote innovation and economic growth.

Sincerely,

Craig D. Spiezle
CEO & President
Online Trust Alliance
Craigs@otalliance.org
https://otalliance.org
+1 425-455-7400

Attachments
Exhibit A IoT Trust Framework 2.0 – Released Jan 2017
Exhibit B - IoT Securing the Internet of Things*; A Collaborative & Shared Responsibility* – March 2017

[16] DIGIT Act https://www.congress.gov/bill/114th-congress/senate-bill/2607

Online Trust Alliance

IoT Trust Framework®

v2.0 - Released Jan 5, 2017

The IoT Trust Framework includes a set strategic principles to help secure IOT devices and their data when shipped and throughout their entire life-cycle. Through a consensus driven multi-stakeholder process, key principles have been identified for connected home, work and wearable technologies including toys and fitness devices. The Framework outlines mandatory requirements including comprehensive and security patching post warranty.

First released in March 2016, version 2.0 of the Framework has been updated to include 37 strategic and measurable principles. These updates incorporate key learnings from field testing, the evolving threat landscape and feedback from industry leaders and related efforts. Core to addressing the inherent security risks and privacy issues is the application of the principles to the entire device solution. These include the device or sensor, the supporting applications, and the backend / cloud services. As many of the products coming to market rely on third party or open source components and software, it is incumbent on developers to apply these principles and conduct supply chain assessments.

Serving as a risk assessment guide for developers, purchasers and retailers, the Framework is the foundation for future IoT certification programs. It is the goal of OTA to post and highlight devices which meet these standards to help consumers, as well as the public and private sectors, make informed purchasing decisions. The Framework and related resources are available for download at https://otalliance.org/IoT.

The Framework is broken down into 4 key areas, including a mix of core requirements (●) and recommendations (❍). The four categories these include:

- **Security Principles** (1-9) – Applicable to any device or sensor and all applications and back end cloud services. These range from the application of a rigorous software development security process to adhering to data security principles for data stored and transmitted by the device, to supply chain management, penetration testing and vulnerability reporting programs. Further principles outline requirements for life-cycle security patching.
- **User Access & Credentials** (10-14) – Requirement of encryption of all passwords and user names, shipment of devices with unique passwords, implementation of generally accepted password re-set processes and integration of mechanisms to help prevent "brute" force login attempts.
- **Privacy, Disclosures & Transparency** (15-30) – Requirements consistent with generally accepted privacy principles including prominent disclosures on packaging, point of sale and/or posted on line, capability for users to having the ability to reset devices to factory settings and compliance with applicable regulatory requirements including the EU GDPR and children's privacy regulations. Required disclosures include the impact to product features or functionality if connectivity is disabled.
- **Notifications & Related Best Practices** (31-37) - Key to maintaining device security is having mechanisms and processes to promptly notify a user of threats and action(s) required. These principles include requiring email authentication for security notifications. In addition messages must be written for maximum user comprehension and tamper-proof packaging and accessibility considerations are recommended.

Note – Highlighted text indicates material changes from version 1.0 released March 2016.

IoT Trust Framework ● Required ○ Recommended	
Security – Device, Apps and Cloud Services	
1. Ensure devices and associated applications support current generally accepted security and cryptography protocols and best practices. 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. All IoT support web sites must fully encrypt the user session, from the device to the backend services. Current best practices include HTTPS or HTTP Strict Transport Security (HSTS) by default, also known as AOSSL or Always On SSL. Devices should include mechanisms to reliably authenticate their backend services and supporting applications.	●
3. 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.	●
4. Establish coordinated vulnerability disclosure including processes and systems to receive, track and promptly respond to external vulnerabilities reports from third parties including but not limited to customers, consumers, academia and the research community. Remediate post product release design vulnerabilities and threats in a publicly responsible manner either through remote updates and/or through actionable consumer notifications, or other effective mechanism(s). Developers should consider "bug bounty" programs, and crowdsourcing methods to help identify vulnerabilities that companies' own internal security teams may not catch or identify.	●
5. Must have a mechanism for automated safe and secure methods to provide software and/or firmware updates, patches and revisions. Such updates 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. Automated (vs automatic) updates provide users the ability to approve, authorize or reject updates	●
6. Ensure all IoT devices and associated software, have been subjected to a rigorous, standardized software development lifecycle process and methodologies 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 across a range of typical use case scenarios and configurations, including preventing any data leaks between the device, apps and cloud services. Developing secure software requires thinking about security from a project's inception through implementation, testing, and deployment. Devices should ship with reasonably current software and/or on first boot push automatic updates to address any known critical vulnerabilities.	●
7. Conduct security, and compliance risk assessments for all service and cloud providers. (See resource guide for recommendations).	●
8. Develop and maintain a "bill of materials" including software, firmware, hardware and third party software libraries (including open source modules and plug ins). (*This would apply to the device, mobile and cloud services to help quickly remediate disclosed vendor or open source vulnerabilities)*	○
9. Design devices to minimum requirements necessary required for operation. For example, USB ports or memory card slots should only be included if they are required for the operation and maintenance of the device. Unused ports and services should be disabled.	●
User Access & Credentials	
10. Include strong authentication by default, including providing 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.	●

IoT Trust Framework ● Required ○ Recommended	
11. Provide generally accepted recovery mechanisms for IoT application(s) and support passwords and/or mechanisms for credential re-set using multi-factor verification and authentication (email and phone, etc.) where no user password exists.	●
12. 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.	●
13. Provide users notification of password reset or change utilizing secure authentication and /or out-of-band notice(s).	●
14. Authentication credentials including but not limited to user passwords shall be salted, hashed and/or encrypted. Applies to all credentials stored to help prevent unauthorized access and brute force attacks.	●
Privacy, Disclosures & Transparency	
15. Ensure privacy, security, and support policies are easily discoverable, clear and readily available for review prior to purchase, activation, download, or enrollment. In addition to prominent placement on product packaging, on their website, it is recommended companies utilize QR Codes, create user friendly short URLs and other similar methods maximizing disclosure at point-of-purchase.	●
16. Disclose the duration and end-of-life security and patch support, (beyond product warranty). Such disclosures should be aligned to the expected lifespan of the device and communicated to the consumer prior to purchase. *(It is recognized IoT devices cannot be indefinitely patched. Consider communicating the risks of using a device beyond its usability date, and impact and risk if warnings are ignored or the device is not retired).*	●
17. 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.	●
18. Disclose what and how features will fail to function if connectivity or backend services becomes disabled or stopped including but not limited to the potential impact to physical security. *(Consider building in controls to disable connectivity or disable ports to mitigate potential threats, while maintaining core product functionality, based on the device usage, balancing out potential life/safety issues).*	●
19. Disclose the data retention policy and duration of personally identifiable information stored.	●
20. IoT devices must provide notice and/or request a user confirmation when initially pairing, onboarding, and/or connecting with other devices, platforms or services.	●
21. Publically disclose if and how IoT device/product/service ownership and the data may be transferred (e.g., a connected home being sold to a new owner or sale of a fitness tracker).	●
22. 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 that 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.	●
23. 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."	●
24. 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.	●
25. 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.	●

IoT Trust Framework ● Required ○ Recommended	
26. 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.	●
27. Comply with applicable regulations including but not limited to the Children's Online Privacy Protection Act (COPPA) and international privacy, security and data transfer regulatory requirements.	●
28. Publicly post the history of material privacy notice changes for a minimum of two years. Best practices include date stamping, redlines, and summary of the impacts of the changes.	●
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 the ability to reset a device and application to factory settings, providing the ability for erasure and zeroization in the event of transfer, loss or sale.	○
Notifications & Related Best Practices	
31. End-user communications including but not limited to email and SMS, must adopt authentication protocols to help prevent spear phishing and spoofing. Domains should implement SPF, DKIM and DMARC, for all security and privacy related communications and notices as well as for parked domains and those that never send email.	●
32. For email communications within 180 days of publishing a DMARC policy, implement a reject or quarantine policy, directing ISPs and receiving networks to reject email which fails authentication verification checks.	○
33. 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.	○
34. Implement measures to help prevent or make evident any physical tampering of devices. Such measures help to protect the device from being opened or modified for malicious purposes after installation or from being returned to a retailer compromised.	○
35. Consider how to accommodate accessibility requirements for users who may be vision, hearing and or mobility impaired to maximize access for users of all physical capabilities.	○
36. Develop communications processes to maximize user awareness of any potential security or privacy issues, end-of life notifications and possible product recalls, including in app notifications. Communications should be written maximizing comprehension for the general user's reading level. *Consider multi-lingual communications recognizing that English may be the "second language" for users (see related principles regarding security and message integrity).*	●
37. Enact a breach and cyber response and consumer notification plan to be reevaluated, tested and updated at least annually and/or after significant internal system, technical and / or operational changes.	●

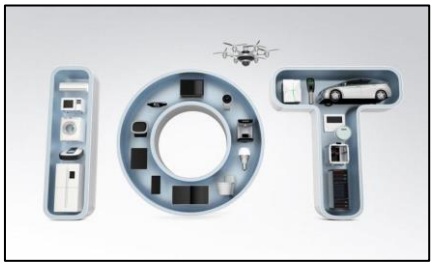
For Updates and resources including the IoT implementation guide visit https://otalliance.org/IoT

Securing the Internet of Things

A Collaborative & Shared Responsibility

Online Trust Alliance

Society and the global economy are witnessing an unparalleled level of innovation being brought forth from the introduction of thousands of new Internet of Things (IoT) connected devices. They are providing significant benefits to the home and office, while wearable devices offer the promise of enhancing one's personal lifestyle and health. Yet to date, the level of commitment to device security, privacy and sustainability is unclear. Many within the security community believe industry is not adequately addressing fundamental security, privacy and life-safety issues. All too many IoT devices appear to be designed primarily for convenience and functionality while long-term security is conspicuously absent. Many of these "smart" devices are often not as smart as suggested.



In the absence of adoption of security norms and responsible privacy practices we are reaching a crossroads where regulation may be required. Yet in reality legislation by itself will not be effective. Passing regulation will take too long and will never keep pace with the evolving threat landscape. With the Trump administration's stated goal to eliminate two regulations for every new one introduced, one should not expect government to solve this problem any time soon. One promising alternative is an inclusive, multi-stakeholder effort that recognizes the need for change and expresses a willingness to adopt self-regulatory frameworks. Self-regulation is not without its own challenges. While well intended, it is often the case that decision makers are not committed and the consensus-driven process results in little if any impactful results.

Much like global warming or industrial pollution, there will be long-term consequences resulting from inaction with IoT threats. The impact of these threats have jumped to the physical world, ranging from unlocking doors, turning on cameras, shutting down critical systems and theft of personal property. The door has been opened. The lack of action has created a treasure chest ripe for abuse by white collar criminals, terrorists and state sponsored actors as IoT devices become weaponized. Left unchecked we may realize a "digital environmental disaster".

CHALLENGES OF THE CONNECTED AUTO, GYM, HOME & OFFICE

Risks to one's personal and physical safety have become reality. All too many connected devices sold, ranging from automobiles and thermostats to children's toys and fitness devices, have insecure remote access and controls. By default many collect vast amounts of personal and sensitive information which may be shared and traded on the open market. The majority of these devices do not have the functionality (or an easily discoverable method) to easily remove one's personal data. Ideally, they would have an "easy button" to reset a device when sold, transferred or rented to others. Such a function should preserve security patches and updates, while deleting user data and disabling any access by the previous owner, remove supporting applications and permanently deleting data on backend services.

Two years ago we sold a home which had a smart thermostat, smart TV and connected garage door openers. No one in the buying or selling process, including the realtors, ever asked about transferring such access to the new buyers. The reality elevated when I sold a car earlier this year. No one suggested the need to delete my mobile app remote access, purge my navigation and trip history, or remove my HomeLink wireless access to my gate or garage. Fortunately we addressed this in advance, but one has to question if the car dealership should have reminded us when taking the car in to trade.

Amplifying the risk are voice commands. There is no doubt Amazon Echo and Google Home offer great functionality. We should expect to see growth in voice enabled device popularity as they propagate throughout the home and office. Yet to date these devices do not have sufficient user authentication. While some devices have options to limit direct purchasing of additional products and services, few if any controls are in place to curb "unauthorized voices" issuing commands. Someone outside of a home yelling through a window, a voice on a TV or even a message left on an answering machine could issue commands such as "open my door" or "turn my heat off." It does not take much imagination to realize the risk and impact of physical harm which could occur.

COLLABORATIVE RESPONSIBILITY TO HELP SECURE IoT

Who is responsible to ensure IoT safety and privacy? What happens when devices can no longer be patched to counter emerging threats? What happens when devices are abandoned by a company going out of business, purchased by another company or the product line is discontinued? Worse yet, what happens when criminals target the installed base of insecure devices?

The reality is both the public and private sectors need to recognize products have a finite security lifespan. At the same time, industry must disclose the duration of their security commitment, ideally as a point of product differentiation. Devices should have the capability to automatically self-check that they are properly configured and secure. When this is not possible, users should be notified and instructed how to disable them. While such devices may continue to function and appear safe to the user, they may no longer be secure and patchable. Expecting the typical user to determine on their own if their devices are insecure and recognize the need discontinue use is unrealistic and places the Internet at-large at risk. In such cases, devices such as the smart coffee maker or thermostat should continue to be able to make coffee and control a home temperature without connectivity, reducing the security and privacy risks and exposure to all parties.

All stakeholders bear a responsibility and opportunity. OTA calls on all parties to demonstrate leadership to help ensure the long-term trust, safety and resiliency of the Internet.

1. **Retailers, Resellers & E-commerce Sites** – The retail channel may be the most influential party holding the keys to change. By establishing minimum security and privacy standards for the products they sell, industry will have to change their design and support practices. Not unlike retailers pledging to not source products made by child labor or those from unsustainable forests, they play a pivotal role in setting baseline product safety measures for the products they profit from. Companies such as Amazon, Best Buy, Costco, Home Depot, Target and others have an opportunity to help drive change while helping to protect society at large. Who will be first?
2. **Developers, Manufacturers & Auto Makers** – Manufacturers need to disclose their security support commitment to users prior to purchase. Not unlike food nutrition labels or new car stickers, they need to clearly articulate their security and privacy policies. Such notices should be included on product packaging and point of sale materials to easily inform the consumer prior to purchase. Adequate notice is not after a smart TV is purchased, hauled home and mounted on the wall. Such disclosures need to be discoverable and articulated in easy to understand terms to let the consumer make an informed purchase decision. As an incentive, companies that adopt sound security principles and embrace responsible privacy practices should not only receive preferential treatment and placement from retailers, but also should get "safe-harbor" from regulators.
3. **Brokers, Builders, Car Dealers & Realtors** – A smart home or connected auto are attractive selling points for every buyer or renter. Often listed as a home or car feature, sellers should be encouraged to disclose all such devices, disable their access, and provide new owners the ability to re-set them. At "closing," car rental or sale they should be required to turn in their physical and digital keys, and remove all personal data. Leading trade groups have taken steps to help address top privacy issues.[1]
4. **Internet Service Providers (ISPs) & Carriers** – Recent incidents of botnets weaponizing and taking control of IoT devices has become a shot across the bow as high-profile websites have been rendered inaccessible. Today in several countries including Australia and Germany, ISPs block botnets emanating from residential IP addresses. Compromised users are placed in "walled gardens," having limited online access to help protect society from harm. While many have recognized this as a best practice, U.S. based ISPs and wireless carriers are not required to take action. In developing related public policy, it is important to recognize ISPs should not have to bear the burden of fixing devices they do not manage or become the consumer's "help desk". Perhaps this is an opportunity for ISPs to expand their security offerings. Who will lead the way?
5. **Regulators & Policy Makers** – Regulators need to recognize there is no perfect security or privacy. To promote innovation and commerce they should encourage self-regulation while providing a "safe-harbor" to device manufacturers who can demonstrate they have adopted reasonable security and responsible privacy practices. Conversely, companies that fail should be "put on notice" that they may be exposed to oversight, fines and or class-action suits.
6. **Consumers** – Consumers must recognize the need to patch and ultimately replace insecure devices beyond their expected security life. Not unlike recycling or having car emissions checked, the benefit is for the greater good of society. When buying a connected device one should review the company's support commitment and privacy policy. If this information is not readily available or if their privacy practices are unacceptable, look for another product. Consumers should not have to risk having their personal information collected, sold and shared in perpetuity without explicit consent.[2] At the same time, opting into such data collection while realizing added benefits may be a fair value-exchange. Informed choice benefits all!

WORKING TOGETHER - DRIVING TRUST & INNOVATION

Looking ahead we have to hope the majority of IoT devices will never be compromised allowing society to realize the promise and scale of IoT. At the same time we need to act today to maximize the security, privacy and vitality of all IoT devices. As devices proliferate the home and office, we need to accept the reality of abuse. As witnessed with recent bot attacks, society and critical infrastructure can and will be damaged from an amplified and sustained attack. As they become proxies for abuse, we need to realize the risk of significant harm to not only our economy, but to the cities where we live and work. This can be averted by working together to enhance security, privacy and resiliency to realize the potential of a connected society. Acting now will help prevent and mitigate the risk of a digital disaster. We all have a role and responsibility to address security and privacy

Recognizing these risks and public policy implications, more than two years ago OTA convened a multi-stakeholder effort. Participants included over 100 organizations including ADT, Center for Democracy and Technology, DigiCert, Device Authority, the Internet Society, the National Association of REALTORS, Microsoft, Symantec, Verisign, TRUSTe and others.[3, 4] Incorporating related efforts from the U.S. Department of Commerce, DHS, FCC, FTC, White House and others, in January 2017 OTA released the IoT Trust Framework 2.0 (https://otalliance.org/IoT). The Framework serves as a comprehensive set of actionable, measurable and most importantly achievable principles for IoT developers.[5,6,7,8] By design it provides prescriptive guidance to embrace security and privacy by design into IoT devices and applications. It not only addresses the security and data privacy when a device is shipped, but most importantly sustainability; how devices can be kept secure over their connected life.[9] In addition OTA has released other resources including the Smart Home and device setup checklists to help maximize the security and privacy of connected devices. See https://otalliance.org/SmartHome.

OTA is a member-driven non-profit think tank with a global mission to enhance online trust, user empowerment and innovation. OTA develops and accelerates the adoption of trust enhancing best practices, and promotes balanced public policy and the importance of meaningful self-regulation. In addition, OTA publishes annual benchmark research including the annual Online Trust Audit (https://otalliance.org/TrustAudit), recognizing leadership in security, data stewardship and responsible privacy practices. To learn more visit https://otalliance.org.

---

[1] Auto Dealers Association www.AutomotivePrivacy.com and National Association of REALTORS https://www.nar.realtor/

[2] See IoT Smart Home and Smart Devices Checklists https://otalliance.org/SmartHome

[3] Internet Society IoT Overview http://www.internetsociety.org/iot (October 2015)

[4] National Association of REALTORS https://crtlabs.org/

[5] FCC https://apps.fcc.gov/edocs_public/attachmatch/DOC-343096A1.pdf (January 2017)

[6] FTC Guidance to help address Security & Privacy Risks https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices (January 2015)

[7] DHS IoT Strategic Principles https://www.dhs.gov/news/2016/11/15/dhs-releases-strategic-principles-securing-internet-things (November 2016)

[8] IoT Trust Framework and key security and privacy principles https://otalliance.org/IoT (January 2017)

[9] NTIA IoT Upgradability & Patching https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security