Statement for the Record

"Understanding the Role of Connected Devices in Recent Cyber Attacks"

United States House of Representatives

Committee on Energy and Commerce

Joint Hearing of the

Subcommittee on Communications and Technology and

Subcommittee on Commerce, Manufacturing, and Trade

By

Craig Spiezle

Executive Director & President

Online Trust Alliance

November 16, 2016

https://otalliance.org

425-455-7400

November 15, 2016

Chairman Walden and Chairman Burgess and Members of the Subcommittees,

Thank you for inviting me to submit a statement to the record regarding how the Internet of Things (IoT) connected devices are being used in cyber-attacks to cause disruption and impact the resiliency of online services. The Online Trust Alliance (OTA) applauds the leadership of the Committee in calling for this hearing.

For background, OTA was formed in 2005 is a 501c3, non-partisan think tank with the mission to enhance online trust, promote innovation and strengthen the integrity and resiliency of online services. Supported by an international coalition of organizations across the public and private sectors, OTA has been a convener bringing together developers, vendors and policymakers to proactively address these challenges, develop best practices, and provide benchmark research.[1]

The following statement provides 1) an overview of the unique security challenges introduced by the proliferation of IoT devices, 2) recommendations to help secure devices and Smart Homes, 3) an overview of the IoT Trust Framework, a set of security and privacy enhancing principles for connected devices, and 4) considerations to help prevent and mitigate the risks associated with products being sold and already in use in homes and businesses worldwide.

Background

The rapid rise in the Internet of Things (IoT) has brought forth a new generation of devices and services representing the most significant era of innovation and growth since the launch of the Internet. IoT solutions are game-changers offering consumers, businesses and governments across the globe countless benefits. From fitness trackers to connected thermostats and toys to “smart” cities and medical devices, society is on the cusp of a new technological era. With this great innovation come significant risks, concerns and responsibilities. While the majority of devices are safe and secure by today’s standards, all too many lack security safeguards, privacy controls, or lifecycle support plans that leave them susceptible for abuse. When combined, these devices have a capacity for causing significant disruption and very real threats to life and safety.

Recognizing the mounting impact to security, privacy and most importantly personal and physical safety, in February 2015 OTA established the IoT Trustworthy Working Group, an inclusive coalition with the mission to develop essential key security and privacy principles and controls to better ensure human and physical safety. This group includes not only technology and privacy leaders such as Microsoft, Symantec, Verisign and TRUSTe, but others including ADT, the National Association of REALTORS, ACT; the App Association, the Houston School District, Guardian Life Insurance, HSB Group as well input from global organizations including the International Telecommunication Union (ITU), the Internet Society and the International Consumer Research & Testing organization.

Recognizing the importance of working with the public sector, over the past year OTA has briefed staff members of this Committee as well as the White House, Federal Trade Commission, Federal Communications Commission, Department of Homeland Security and the Department of Commerce.

We believe the recent Distributed Denial of Service (DDoS) attacks which have been increasing dramatically in frequency and scale since September, have been a “shot across the bow” and we need to prepare for the worst. Just last week, a similar attack led to the disruption of heating systems in the city of Lappeenranta Finland, leaving thousands of residents in subzero weather by disabling a central heating system.[2] Researchers and malicious actors continue to demonstrate ways an insecure IoT device can drive collective harm in the physical world. These include the ability to distribute ransomware, overheat

[1] Online Trust Alliance https://otalliance.org

[2] DDOs Attacks Central Heating System http://thehackernews.com/2016/11/heating-system-hacked.html

devices with the potential for causing fires and disabling security systems. As witnessed in all too many data breaches the fundamentals of IoT "security and privacy by design" are often overlooked.[3] [4]

Unique Challenges

The IoT ecosystem is made up of three dimensions: the device or sensor, the supporting applications, and the backend / cloud services. Combined with the supply chain of each, every facet and data layer is a potential risk. Each needs to be secured across multiple layers as does the flow of data between them. If the integrity of the data or device is compromised, connectivity interrupted, or the functionality remotely controlled by a malicious actor, the consequences can and will be catastrophic.

Incorporating security and privacy protections in the earliest stages of design is the most effective way to bring secure IoT devices to market and to help ensure their safety tomorrow. The processes, technologies and policies that protect users require ongoing support throughout the device's life. Support post-warranty (including usability, patch management, data ownership and portability) must be addressed. Defined as "sustainability," it is the risk and implications of devices left unpatched, orphaned (no longer supported), or bricked (disabled if the company shuts down the apps or backend service). Sustainability also includes the policy issues related to the ownership and transferability of the device and user data. Since devices may outlive an owner or be transferred to new home buyers, consumers and businesses need the assurance that companies will continue to address these needs post warranty. Continuing use of out-of-date devices abandoned or orphaned by their manufacturer will render them insecure and at risk of being targeted and exploited.

Still, it is important to recognize there is no perfect security and privacy and all products have a finite security lifespan. One example is Windows XP. In spite of Microsoft providing Windows XP users no-charge support for over a decade, today millions of PCs running XP remain at risk.[5] While such legacy devices may be secure when shipped, no degree of patching can address unforeseen threats decades later.

Shared Responsibilities: What We Can Do Today & Tomorrow

To address these combined issues, OTA convened a cross industry working group with the vision to develop best practices and create an IoT Trust Framework, a voluntary self-regulatory model. While this effort was in review, the OTA and National Association of REALTORS released the Smart Home checklist in October 2015 to help educate consumers and the real estate industry regarding the issues and risk of their devices and the connected home (see Exhibit B).[6]

The Framework was released this past March, identifying 31 criteria initially focused on the connected home, office and wearable technologies (Exhibit C).[7] Serving as a voluntary code of conduct, the Framework is the foundation for several certification and risk assessment programs in development. Further, the Framework is a tool to help assess security and privacy risks for retailers, home builders and businesses regarding the products they may sell, install and purchase.

Collectively, we have a shared responsibility to help protect the security and privacy of individuals, enterprises, and the nation. The Framework represents a major step to help shape products being developed, but we also need to consider what we can do to help address the risks in products being sold today and in use worldwide. We recommend the Committee to call on stakeholders to consider these initial guidelines. Where technically and economically feasible, these and other efforts are needed so together, we may build a safer, more secure world and enable the IoT industry to reach its full potential.

[3] OTA Research September 8, 2016 https://otalliance.org/IoTvulnerabilities
[4] 2016 Data Breach Readiness Guide https://otalliance.org/Breach
[5] Windows XP Support https://support.microsoft.com/en-us/help/14223/windows-xp-end-of-support
[6] https://otalliance.org/smart-home
[7] https://otalliance.org/news-events/press-releases/ota-releases-iot-trust-framework

Recommendations to Help Secure Devices Being Sold & In Use

1. **Developers and manufacturers**
   a. Proactively communicate to customers any security and safety advisories and recommendations.
   b. Products which can no longer be patched and have known vulnerabilities should either have their connectivity disabled, the product recalled and/or the consumers notified of the risk to their personal safety, privacy and security of their data.
   c. Provide disclosures, including on product packaging, stating the term of product / support beyond the product warranty.
   d. Update websites to provide disclosures and security advisories in clear, everyday language.
2. **Retailers / Resellers / eCommerce Sites**
   a. Voluntarily withdraw from sale products being offered without unique passwords or without a vendor's commitment to patching over their expected life.
   b. Apply supplementary labels or shelf-talkers advising buyers of products with exemplary security data protection and privacy policies.
   c. Notify past customers of recalls, security recommendations and of potential security issues.
3. **Consumers and users** have a shared responsibility. Users need to
   a. Maintain devices and stay up to date on patches.
   b. Update contact information including email address for all devices.
   c. Regularly review device settings and replace insecure and orphaned devices (see Exhibit A).
4. **ISPs** should consider the ability to place users in a "walled garden" when detecting malicious traffic patterns coming from their homes or offices. In concept this would allow basic services such as 911 access and medical alerts, while limiting other access. Such notifications can advise consumers of the harm being incurred, and the need to make changes, replace devices or seek third party support. It is important to clarify as outlined by the FCC's Communication Security & Reliability Council in 2012, such notifications should not directly burden ISPs or carriers to remedy the problem unrelated to their services provided.[8]
5. **Government**
   a. Fund outreach and education, working with trade organizations, ISPs, local grassroots organizations, media, State Agencies and others to raise awareness of the threats and responsibilities. Focus on teachable moments such as at time of purchase, inclusion in billing statements and emails to installed base of users and notices to ISP customers.
   b. Prioritize "whole-of-government" approach to the development, implementation, and adoption of efforts and initiatives, with a global perspective. Coordinated efforts will help to ensure industry can innovate and flourish while enhancing the safety, security, and privacy of consumers, enterprises, and the nation's critical infrastructure.

Working Together

The future of IoT cannot be realized without addressing security, data privacy and life-safety issues. Making security and privacy part of every product's feature set and designing it in from the onset is a shared responsibility for both the public and private sectors. Creating a culture of security, privacy and sustainability with transparency will yield long-term benefits to society. OTA looks forward to working with members of the Committee to accelerate the development of best practices, including core safety and privacy requirements, to realize the potential of IoT while promoting safety and privacy innovation helping to protect our economy and society from abuse.

[8] See FCC Anti-Botnet Code of Conduct for ISPs and related recommendations http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG7-Final-Report.pdf

Exhibit A

Online Trust Alliance

Enhancing the Security, Privacy & Safety of Connected Devices

Addressing cyber threats, identity theft and personal safety risks	
❑	Inventory all devices within your home and workplace that are connected to the Internet and network. Router reports can help determine what devices are connected to your network. Disable unknown and unused devices.
❑	Contact your Internet Service Provider (ISP) to update routers and modems to the latest security standards. Change your router service set identifier (SSID) to a name which does not identify you, your family or the device.
❑	Check that contact information for all of your devices are up-to-date including an email address regularly used to receive security updates and related notifications.
❑	Confirm devices and their mobile applications are set for automatic updating to help maximize protection. Review their sites for the latest firmware patches and updates.
❑	Review all passwords creating unique passwords and user names for administrative accounts and avoid using the same password for multiple devices. Delete guest codes no longer used. Where possible implement multi-factor authentication to reduce the risk of your accounts being taken over. Such protection helps verify who is trying to access your account—not just someone with your password.
❑	Review the privacy policies and practices of your devices, including data collection and sharing with third parties. Your settings can be inadvertently changed during updates. Reset as appropriate to reflect your preferences.
❑	Review devices' warranty and support policies. If they are no longer supported by the vendor, disable the device's connectivity or discontinue usage of the device.
❑	Before discarding, returning or selling any device, remove any personal data and reset it to factory settings. Disable the associated online account and delete data.
❑	Review privacy settings on your mobile phone(s) including location tracking, cookies, contact sharing, bluetooth, microphone and other settings. Set all your device and applications to prompt you before turning on and sharing and data.
❑	Back up your files including personal documents, financial records, music and photographs to storage devices that are not permanently connected to the Internet.

https://otalliance.org/IoTconsumer

Online Trust Alliance

Exhibit B

NATIONAL ASSOCIATION of REALTORS®

SMART HOME CHECKLIST

Maximizing security & privacy in your connected home

PRIOR TO OCCUPANCY / CLOSING	
❑	Obtain inventory and documentation of all connected devices including but not limited to manuals, vendor / manufacturer contacts and websites. Examples of connected devices include: ❑ Modems, gateways, hubs, access points ❑ Connected access for garage, locks, gates ❑ External keypads for garage, locks, gates ❑ Thermostats, HVAC, energy systems ❑ Smart lighting systems ❑ Smoke, carbon monoxide, etc. detectors ❑ Sprinkler / irrigation systems ❑ Appliances (TV, refrigerator, washer/dryer, etc.) ❑ Auto controls linked to home systems ❑ Security alarms, video monitoring systems
❑	Review privacy and data sharing policies of all devices and services.
❑	Obtain confirmation from previous occupants and vendors they no longer have administrative or user access.

ALL SMART HOME DEVICES & APPLICATIONS	
❑	Submit change of ownership and contact information to device manufacturers and service providers (email addresses, cell phone numbers, etc.) to ensure you receive security updates and related notifications to maximize your security and privacy.
❑	Review devices' warranty and support policies. Occupants should consider disabling devices or specific features that are no longer supported by a vendor.
❑	Review the configuration settings for remote access, encryption and update cycles and adjust where needed.
❑	Reset privacy and data sharing settings to reflect your preferences. For example – data collection and sharing, camera and microphone settings and other device functions.

MODEMS, GATEWAYS & HUBS	
❑	Review home Internet routers and devices to ensure they support the latest security protocols and standards and disable older insecure protocols.
❑	Update and modify all system passwords and user names upon taking possession of your new home or rental unit. Where possible create unique passwords and usernames for administrative accounts.
❑	Run updates and contact manufacturers to confirm devices are patched with the latest software and firmware.

SECURITY ALARMS, KEYLESS ENTRY, GATE SYSTEMS, ETC.	
❑	Reset access and guest codes for gates and garage door openers.

HOME THERMOSTATS, HVAC SYSTEMS, SMART TVS, LIGHTING & OTHER DEVICES	
❑	Disable connectivity for devices no longer supported by the manufacturer or replace these devices.
❑	Review the privacy practices of the connected devices including data collection and sharing with third parties and reset permissions as appropriate.

Exhibit C

Online Trust Alliance

OTA IoT Trust Framework

IoT Trust Framework ● Required ○ Recommended N/A – Not Applicable	
1. Ensure devices and associated applications 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 user passwords shall be salted, hashed and/or encrypted.	●
3. 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.	●
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 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).	●
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. 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.	●
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.	○
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.	●

IoT Trust Framework ● Required ○ Recommended N/A – Not Applicable	
12. 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.	●
13. 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 and/or after significant internal system, technical and / or operational changes.	●
16. 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 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 stored.	●
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 and the data 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 selling or transfering 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.	●

IoT Trust Framework ● Required ○ Recommended N/A – Not Applicable	
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. Comply with applicable international privacy, security and data transfer regulatory requirements.[9]	●
29. Publicly post the history of material privacy notice changes for a minimum of two years, including date stamping, redlines, and summary of the impacts of the changes.	○
30. 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.	○
31. Provide device or service data erasure and zeroization in the event of transfer, loss or sale.	○

Updates to the Framework, and supporting resources are posted at https://otalliance.org/IoT

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."
2. It is expected companies disclose of sharing data with law enforcement and reference any applicable transparency reports as legally permitted.
3. Smart devices refer to devices (and sensors) which are networked and may only have one-way communications.
4. Smart Cars including autonomous, self-driving vehicles as well as medical devices and HIPPA data[10] are beyond the scope of the Framework, yet the majority of the criteria are deemed to be applicable. Respectively they fall under regulatory oversight of the National Highway Traffic Safety Administration (NHTSA) and the Food and Drug Administration, (FDA). [11]

[9] Companies, products and services must be in compliance with any law or regulation of the jurisdiction that governs their collection and handling of personal and sensitive information, including but not limited to the adherence to the EU-US Privacy Shield Framework www.commerce.gov/privacyshield and/or the EU General Data Protection Regulation (GDPR) www.eugdpr.org. Failure to comply constitutes non-compliance with this framework and would result in the automatic disqualification from any code of conduct or certification program.

[10] U.S Department of Health & Human Services, Health Information Privacy http://www.hhs.gov/hipaa/index.html

[11] http://www.nhtsa.gov/Vehicle+Safety and http://www.fda.gov/MedicalDevices/default.htm