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