Online Trust Alliance

Internet of Things Trust Framework– Discussion Draft

Revised June 10, 2015 - For updates visit https://otalliance.org/IoT

The Internet of Things (IoT) moniker is being applied to 1000's of devices, offering increased utility, functionality and a wide range of consumer and business benefits. Yet, in this rapid race to bring products to market, all too many lack basic security protocols, privacy considerations and related safeguards. . OTA's 2015 Online Trust Audit revealed 14% of leading IoT products lack discoverable privacy policies. Of the 84% who had posted policies, only 10% had short layered notices, only 8% offered policies in multiple languages and none honored "Do Not Track" user requests.[1, 2] Increasingly IoT solutions rely on a mix of third party apps, platforms and cloud services which amplify the data securitys. While it is recognized there is no "perfect security" or "absolute privacy", the lack of standards and controls increases the potential for exploits, data breaches and abusive data use policies to consumers and businesses worldwide.[3]

Recent studies of IoT devices have revealed that devices are increasingly being exposed to vulnerabilities. While many of these short comings have since been addressed by leading websites and mobile app developers, disappointingly many IoT vendors have yet to follow or learn from history. In Symantec's "Insecurity in the Internet of Things" report analyzing IoT devices, widespread security concerns were discovered.[4] Further review confirms widespread location tracking is occurring without consumer consent.[5] As reported by the National Security Telecommunications Advisory Committee's report it determined that there is a rapidly closing window to ensure that IoT standards and practices are adopted in a way that maximizes security and minimize risk. The report concluded "If the country fails to do so, it will be coping with the consequences for generations." [6, 7]

As consumers acquire IoT devices, the security and privacy risk is amplified with every additional device connected to the user's personal and business network. The implications range from identity theft and personal security compromises to data breaches and system compromises. With the forecast of 50 billion IoT connected things by 2020, the impact can be significant.[8]

Retailers are equally as perplexed in their attempt to evaluate which products to merchandise and recommend. In recent interviews with retailers conducted by OTA during RSA 2015, many cited concerns being liability for selling products which might violate consumer protection regulations and security best practices. Equally as concerning is the risk of consumer remorse resulting from data practices, product performance and end-of-life support resulting in product returns.[9]

---

[1] Honor Roll methodology https://otalliance.org/initiatives/2015-honor-roll-methodology

[2] Do Not Track - http://donottrack.us/

[3] www.darkreading.com/rsa-highlighted-impending-iot-troubles/d/d-id/1320191

[4] www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/insecurity-in-the-internet-of-things.pdf

[5] www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/how-safe-is-your-quantified-self.pdf

[6] www.pcmag.com/article2/0,2817,2482620,00.asp

[7] www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20the%20Internet%20of%20Things%20Nov%202014%20%28updat%20%20%20.pdf - November 2014

[8] http://www.mobileworldlive.com/ericsson-backtracks-2020-vision-connected-devices

[9] OTA interviews completed between April 15 - 24, 2015.

In January 2015, the Federal Trade Commission in their Internet of Things report; Privacy and Security in a Connect World, outlined a variety of privacy and security risks which could be exploited to harm consumers. This report highlighted four Fair Information Practices Principles ("FIPPs") including: 1) security, 2) data minimization, 3) notice, and 4) choice.[10] The staff encouraged companies to implement "security by design" on the onset, ensure their personal practices promote good security, retain service providers of maintaining reasonable security and implement defense-in-depth security practices.

In Consumer Report's June IoT issue, they identified several concerns outlining data collection and lack of security practices. They stated IoT devices need to clearly tell consumer about the information being collected and how their information may be shared, sold and used. Unfortunately with the lack of standards consumers are somewhat on their own stating "the best consumer protection advocates may be consumers themselves." [11]

The collective impact from hundreds of thousands of devices malfunctioning simultaneously could divert first responders and overwhelm infrastructure, allowing criminals to victimize other higher value targets. Many national leaders including Michael Daniel, the national cybersecurity coordinator and assistant to the President have suggested the need for a voluntary program, akin to UL testing be established.[12]

Next Steps

Addressing the mounting concerns and collective impact of connected devices, the OTA established the IoT Trustworthy Working Group (ITWG), a multi-stakeholder initiative. The goals of the ITWG is to develop a framework, focusing on voluntary best practices in security, privacy and sustainability. Recognizing the potential broad scope of the "Internet of Everything" the initial focus is limited to two primary categories; 1) home automation and connected home products, and 2) wearable technologies; limited to health & fitness categories. While many participants recognize other categories as equally or potentially of greater importance, automotive technologies, HIPAA and FDA related devices are out of scope as they are regulated by other entities.

A recurring concern raised by participants of the ITWG is the need for practical disclosures that are provided to consumers prior to acquisition of products and services, as well as some to be determined frequency of recurring notices of the data practices. Working group members believe devices should be prohibited from using spoken words, images or other sounds for any purpose not essential to the function of the application or device and such voice or image recognition features be disabled by default, requiring user consent for activation.

Recognizing the need for "responsible data security and privacy practices" (aka data stewardship), participants of the ITWG support the concept of the "law of least data" where data collection and flows are minimized. For example should some have suggested a home thermostat should connect directly to the HVAC system without the need to pass data to from a cloud service. Not only does this minimize security and privacy issues, it improves resiliency while also reducing the risk of performance latency.

The group further recommends that security and privacy by design must be a priority from the onset of product development. ITWG supports the investigation and development of a certification program evaluating devices and applications against published criteria. The ITWG acknowledges all criteria must be transparent, be vendor and technology neutral, and approach the program goals holistically. In concept, certification and compliance would be verified through a combination of self-certification and third party auditing against a set of published criteria and company assertions. Such a program requires funding for program development and management, testing, consumer and business education, legal review, logo development, licensing, and ongoing monitoring and compliance enforcement. ITWG welcomes support from both the public and private sector.

---

[10] FTC IoT Report www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

[11] www.consumerreports.org/cro/magazine/2015/06/privacy-tips-for-the-internet-of-things/index.htm

[12] www.darkreading.com/vulnerabilities---threats/white-houses-daniel-intrigued-by-ul-type-model-for-iot-security/d/d-id/1320057

Consumers need to know / expect:

1. Does my device / application have a posted privacy policy which respects my data and privacy?
2. Can I opt-in or opt-out and what will the impact be to the product functionality?
3. Does the manufacturer and app developer follow a Security Development Lifecycle (SDL).
4. Is my data protected at rest and in transit?
5. Does my device have a published support policy including end of life?
6. How will my device be upgraded to address security vulnerabilities? How will I be notified?
7. How can my data be deleted if the device is lost, stolen or sold?
8. How can I compare security and privacy practices as part of my purchase decision?
9. Does the manufacturer share or monetize my data?
10. What is the risk my personal data could be re-identified?

Framework Goals:

1. Provide guidance to manufacturers and developers to help reduce attack surface and vulnerabilities, and adopt responsible privacy and data stewardship practices.
2. Drive the adoption of security, privacy & sustainability best practices; embracing "privacy and security by design", as a model for the development of voluntary, yet enforceable code of conduct. [13]
3. Provide positive affirmation and recognition to companies, products, and retailers who embrace the code of conduct and meet minimum standards.
4. Provide retailers / commerce sites criteria to aid in their product merchandising and promotion decisions.
5. Where possible, apply existing standards from NIST, NTIA, ISO and other industry working groups. [14]
6. Encourage collaboration, sharing of best practices and threat intelligence.
7. Evaluate and identify gating issues and considerations which may lead to the development of a seal or certification program which could become an incentive to adopt best practices. [15]

[13] Companies who assert data security and privacy practices would likely be held accountable by section 5 of the FTC Act and related State consumer protection regulations. www.ftc.gov/enforcement/statutes/federal-trade-commission-act

[14] www.iso.org/iso/home.html

[15] See Online Trust Audit and Honor Roll as example of a program recognizing best practices https://otalliance.org/HonorRoll

Key Program Pillars [16]

- Security
- Privacy
- Sustainability (including upgradability, supportability and end-of-life)

Responsible Data Privacy

1. Is the privacy policy publically available to review prior to product purchase or activation? (Is it visible on packaging, POS materials…)
2. Is the privacy policy display optimized for the user interface. For example is a short-layered notice applicable and discoverability and with access to the complete notice.
3. Is data sharing limited to third parties / service providers who agree to confidentiality and limit usage to support product features/ functionality and or product improvement?
4. Can a user opt-In for any third party data sharing; not contingent on utilizing of core features or updates?
5. Can the consumer see or request access to the data and analytics (and the specific data attributes) that has been collected from their device? Are all data elements attributed to a user clearly disclosed and explained? What is feasible to provide?
6. Is a data retention policy disclosed, including the provision of user information being deleted upon termination of product usage or product end-of-life?
7. Does the vendor make a commitment to not transfer any consumer data if the company is sold or liquidated unless the consumer is provided notice and gives express consent (with the exception of data required to perform product support and functionality as specified in the original product terms of use and privacy policy)?
8. Is it COPPA compliant? Who is the user? When does it apply? Do user profiles need to be created? [17]
9. What steps are taken to help prevent anonymous data being from being re-identified?
10. Can a consumer return a product without any charge after reviewing the privacy practices that might be presented during set up? (retailer or product policy).
11. Can the company materially change privacy policies after the product is purchased? What is the primary function of the device and how might it be impacted? Is the history of changes available for review and or comparison? [18]
12. Is the device compliant with regulations where the device is being sold or being used? (US vs Canada, UK, Australia and or EU?

[16] *Same criteria may not be applicable to the connected home or wearables based on the data or application*

[17] https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule

[18] See example of best practices http://www.google.com/policies/privacy/archive/

Security

1. Does the device have controls and documentation enabling the consumer to set and manage privacy and security preferences including what information is transmitted via the device.
2. Is personal data encrypted or hashed at rest and in motion using best practices including connectivity to mobile devices including Wi-Fi and Bluetooth connectivity?[19]
3. Are default passwords and user names randomly generated; prompted on first use?
4. Has their website or API adopted HSTS or AOSSL (or equivalent technologies) to help prevent session jacking and eavesdropping by wireless hotspots or third parties? (key to connect to cloud services) [20]
5. How does their site security score? Does it adhere to SSL best practices? [21]
6. All consumer email communications adopt email authentication protocols including SPF, DKIM and DMARC to counter email fraud and spear phishing? [22]
7. Does the vendor have remote capabilities to remediate threats in a prompt and reliable manner? (Does it require user interaction?) What are the risks?
8. Does the vendor have a breach response and consumer safety notification plan? [23]
9. Has penetration testing been verified including devices, application and 3rd party service providers?
10. What notification processes are in place to notify a user of security patches? (connected home)

Sustainability (including upgradability, supportability and end-of-life)

1. Does the company have a recycle and or upgrade program?
2. What is the end-of-life policy?
3. Does the vendor have phone or live chat support?
4. Is my data portable (as applicable)?
5. What are their patch management, recall / consumer notification processes?
6. Can all of the data be easily wiped and re-formatted?
7. Is the device compatibility to technical standards and can the data be downloaded in a non-proprietary format?

This document reflects rough consensus from the Online Trust Alliance IoT Trustworthy Working Group, (ITWG). The Online Trust Alliance (OTA) is a 501c3 charitable non-profit with the mission to enhance online trust while promoting innovation and the vitality of the Internet. Its goal is to help educate businesses, policy makers and stakeholders while developing and advancing best practices and tools to enhance the protection of users' security, privacy and identity. OTA supports collaborative public-private partnerships, benchmark reporting, and meaningful self-regulation and data stewardship. Membership is open to any entity upon application. To learn more, contact the Online Trust Alliance at 425-455-7400 or email admin@otalliance.org.

---

[19] https://www.bluetooth.org/en-us

[20] https://otalliance.org/AOSSL

[21] https://ota.ssllabs.com

[22] https://otalliance.org/DMARC

[23] https://otalliance.org/Breach