Online Trust Alliance

IoT Trust Framework – Discussion Draft

released August 11, 2015 (updated August 13)

As consumers and businesses increasingly rely on IoT devices, the security and privacy risk is amplified. Addressing the mounting concerns and collective impact of connected devices, in January 2015 the Online Trust Alliance, a 501c3 non-profit organization and think tank, established the IoT Trustworthy Working Group (ITWG), a multi-stakeholder initiative. The goal of the ITWG is to develop a framework, focusing on voluntary best practices in security, privacy and sustainability. The initial focus is on two primary categories; 1) Home automation and connected home products, and 2) wearable technologies, limited to health & fitness categories.

As a guiding principle, the framework has been developed to apply to all connected home and wearable products. Recognizing technical limitations due to embedded firmware, some of the requirements may not be applicable to every product or feasible based on the product design. Representing the input of nearly 100 participants, broad consensus is reflected in the framework, yet it is acknowledged there are use cases where consensus is pending.

The fundamental principles underlying the recommendations are based on the Fair Information Practice Principles (FIPPs), notably transparency and data security.[1] This work builds on the data security and privacy best practices advocated by the OTA, recommended by the U.S Federal Trade Commission and highlighted in the OWASP Internet of Things security project.[2, 3, 4]

Security and privacy by design must be a priority from the onset of product development and be addressed holistically. It must be a forethought versus an afterthought, focusing on end-to-end security and privacy.

Working towards the goal of maximizing consumer trust, the 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. The trust framework will evolve over time to reflect the latest best practices, security standards, regulatory requirements and the changing threat landscape. While threats to data may transform over time and new standards and best practices will emerge, the fundamentals of sound security and privacy will remain constant.

The draft framework is presented below. The goal of the working group is to solicit broader feedback leading to the formal release of the framework. To submit comments please visit https://otalliance.org/IoT. The deadline for submissions is September 14th.

[1] FIPPs are the widely accepted framework of defining principles to be used in the evaluation and consideration of systems, processes, or programs that affect individual privacy. These principles are at the core of the Privacy Act of 1974 and are mirrored in the laws of many U.S. states, as well as in those of many foreign nations and international organizations.

[2] https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business

[3] https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project

[4] https://otalliance.org/system/files/files/initiative/documents/ota_iot_trustworthy_framework-draft.pdf

PROPOSED MINIMUM REQUIREMENTS – IoT TRUST FRAMEWORK

The following requirements are the proposed baseline for any self-regulatory and/or certification program. It should be noted in addition to what is outlined below, companies must adhere to all regulatory requirements as they pertain to where their users or consumers reside, including but not limited to breach notification, disclosure requirements, child protection, anti-spam and related consumer protection laws and regulations.

1. **The privacy policy must be readily available to review prior to product purchase, download or activation and be easily discoverable to the user. Such policies must disclose the consequences of declining to opt-in or opt-out of policies, including the impact to usage of key product features or functionality**. Solution may include a short notice on product packaging, point-of-sale materials as well as a link to online privacy policy. It is recommended a link to the privacy policy be on the header and/or footer of every page including product registration page and application download page. The working group acknowledges the need to have flexibility in how and when notices are provided. In some cases notices may be provided on first use or when activating a new feature or within the welcome information packet included with physical product.

2. **The privacy policy display must be optimized for the user interface to maximize readability.** The working group recommends all policies be designed utilizing a short-layered format and recognizes the user interface may be limited for readability, requiring the user to review and consent using another device.[5]

3. **Manufacturers must conspicuously disclose all personally identifiable data types and attributes collected.** For example a health or fitness band would potentially disclose physical location, tracking and personal vitals (heart rate, pulse, blood pressure), as well as user profile data.

4. **Any default personal data sharing must be limited to third parties/service providers who agree to confidentiality and to limit usage for specified purposes.** Acceptable usage would be limited to support product features and functionality; product improvement; or delivery of services on behalf of the application developer or manufacturer. Any sharing of personal data with third parties for other purposes must be disclosed and require opt-in, including an explanation of the nature and scope of the data shared and limitations on the use of the data if any. This requirement places the responsibility on the manufacturer to manage their third party service providers to comply.

5. **The term and duration of the data retention policy must be disclosed.** In general, data should be retained for as long as the user is using the device, or to meet legal requirements. It is acceptable for the policy to state data will be retained as long as a customer uses the product or service and must be deleted upon expiration or account termination.

[5] http://www.truste.com/blog/2011/05/20/layered-policy-and-short-notice-design/

6. **Manufacturers must disclose if the user has the ability to remove, have purged or made anonymous personal and sensitive data (other than purchase transaction history) upon discontinuing device use, loss, damage, sale or device end-of-life.** The working group believes this capability should be provided at no-charge.

7. **Personally identifiable data must be encrypted or hashed at rest (storage) and in motion using best practices including connectivity to mobile devices, applications and the cloud utilizing Wi-Fi, Bluetooth and other communication methods**. As a best practice the goal is to achieve end-to-end encryption of all personal data. Note this would not apply to direct wired connections of the device. This requirement requires the use of current encryption technologies solutions currently being deployed by industry.

8. **Default passwords must be prompted to be reset or changed on first use or uniquely generated.** Where possible, separate passwords should be required for administrative vs user access and not permit password reuse. Ideally passwords should be randomly generated.

9. **All user sites must adhere to SSL best practices using industry standard testing mechanisms**. For example the working group suggests sites score a minimum of 90% using industry benchmark testing tools.[6]

10. **All device sites and cloud services must utilize HTTPS encryption by default.** Also referred to as HTTPS everywhere or Always On SSL (AOSSL). Recognizing the importance of HTTPS, Google has issued an advisory for all consumer facing websites and the White House has mandated that all U.S. government agencies implemented it by December 31, 2016.[7, 8, 9]

11. **Manufacturers must conduct penetration testing for devices, applications and services.** The objective is to help identify and patch vulnerabilities. Ideally such testing should be independently verifiable.

12. **Manufacturers must have capabilities to remediate vulnerabilities in a prompt and reliable manner either through remote updates and / or through consumer notifications and instructions.** Alternatives could be device replacement or manufacturer upgrade, product recall or onsite service for connected home devices**.** *It is recognized some embedded devices' current design may not have this capability and it is recommended such update / upgradability capabilities be clarified to the consumer in advance of purchase.*

13. **Manufacturers must have a breach response and consumer safety notification plan, at a minimum reviewed semi-annually.** Recommended best practices including conducting employee training programs and "tabletop" or breach simulation exercises.[10]

---

[6] See OTA Online Trust Audit https://otalliance.org/HonorRoll and SSL test tool https://ota.ssllabs.com

[7] Always On SSL https://otalliance.org/AOSSL

[8] Google support of HTTPS http://googlewebmastercentral.blogspot.com/2014/08/https-as-ranking-signal.html

[9] https://www.whitehouse.gov/sites/default/files/omb/memoranda/2015/m-15-13.pdf

[10] See Breach Response Planning Guidelines https://otalliance.org/Breach

14. **Manufacturers must provide secure recovery mechanisms for passwords**. Suggestions include multi-factor verification (email and phone, etc.) as well as incorporate lockout capability for multiple sign-on attempts.

15. **Device must provide a visible indicator or require user confirmation when pairing or connecting with other devices.**

16. **All updates, patches, revisions, etc. must be signed/verified.** Such signing helps to insure the integrity of the patch and to verify the source or developer.

17. **For products and services which are designed to be used by multiple family members and collect PII, manufacturers need to incorporate the capability for creating individual profiles and/or have parental or administrative level controls and passwords.**

18. **Manufacturers must publish and provide timely mechanisms for users to contact the company regarding issues including but not limited to the loss of the device, device malfunction, account compromise, etc**.

19. **Manufacturers must provide a mechanism for the transfer of ownership including providing updates for consumer notices and access to documentation and support**.[11]

20. **The device must have controls and/or documentation enabling the consumer to set, revise and manage privacy and security preferences including what information is transmitted via the device.** Capabilities should include ability to reset to the "factory default."

21. **Manufacturers must publish to consumers a time-frame for support after device/app is discontinued or replaced by newer version.** This is recommended beyond traditional warranty policies and should be for the life of the device.

22. **Manufacturers must disclose what functions will work if "smart" functions are disabled or stopped**. Core functions must remain operative in the event the smart component is disabled. For key home automation products, company must provide a backup mechanism for access and use in the event of loss of connectivity (e.g., door openers, garage doors).

23. **Configure all security and privacy related email communications to adopt email authentication protocols**. Current standards include SPF, DKIM and DMARC which aid in the ability counter email fraud, malicious emails and spear phishing exploits.[12] Additionally organizations should consider STARTTLS and opportunistic Transport Layered Security (TLS) for email to aid in securing communications and enhancing the privacy and integrity of the message.[13, 14]

[11] High importance for any connected home device.

[12] See Email Authentication protocol overview and resources https://otalliance.org/eauth

[13] STARTTLS for email https://en.wikipedia.org/wiki/STARTTLS

[14] See TLS for Email - https://otalliance.org/best-practices/transport-layered-security-tls-email

ADDITIONAL RECOMMENDATIONS

The following is a preliminary list of recommendations and considerations organizations may wish to consider above and beyond those outlined in the framework. It is recognized that some of the following may be not be applicable to every device or service.

1. Make a commitment to not transfer any consumer data unless it is a dependent part of the sale or liquidation of the core business which originally collected the data, or unless company has taken reasonable steps to provide consumer notice and consent to such transfer (with the exception of data required to perform product support and functionality as specified in the original product terms of use and privacy policy).

2. Take steps to help prevent personal data from being re-identified.

3. Adhere to the Fair Information Practice Principle of minimal data collection.

4. Disclose if personal data is being stored and accessed in the cloud. For example does the manufacture of a connected thermostat collect the time of temperature changes?

5. Agree to not materially change privacy policies after the product is purchased without consumer consent, providing the core product functionality is not impacted.

6. Provide history of privacy notice changes available for review and or comparison.[15]

7. Plan for the need to include support for evolving protocols/standards.

8. As applicable, require third-party installers be trained to configure devices per security and privacy best practices such as usage of randomly generated usernames and passwords.

9. Provide the ability for a consumer to return a product without charge after reviewing the privacy practices that are presented during initial set up. Such policies should be consistent with current exchange policies of the retailer and or industry.

10. Disclose if the personal data is portable and compatible to common technical standards in a non-proprietary format.

11. Provide configuration roll-back capability in the event a non-security related upgrade conflicts with other connected devices.

12. Manufacturers should optimize the device interface and usability for users with vision, hearing and mobility limitations to maximize use and access for users of all ages and physical capabilities.

[15] See Google's archive http://www.google.com/policies/privacy.