OTA
Online Trust Alliance

OTA IoT Trust Framework – Pre-Release Draft 11/23/2015

The Internet of Things has the potential to transform the way we live, work and communicate. By all accords the growth in IoT connected devices will provide significant benefits, yet as they proliferate, the security and privacy risks are amplified. Left unchecked, society could be faced with scenarios where 100,000s of devices are compromised simultaneously, creating panic and disrupting first responders.

Addressing the mounting concerns, in January 2015 the Online Trust Alliance established the IoT Trustworthy Working Group (ITWG), a multi-stakeholder initiative. For purposes of this report, the term IoT refers to “things” such as devices or sensors – other than computers, smartphones, or tablets – that connect, communicate or transmit information with or between each other through the Internet. The group recognizes that “security and privacy by design” must be a priority from the onset of product development and be addressed holistically. Devices and applications should be built with privacy and security protections that are commensurate with the risk posed to the end user. The framework focuses on privacy, security and sustainability, including a defense-in-depth strategy for all systems. Sustainability is critical as it looks at the life cycle issues related to long- term supportability and transfers of ownership of devices and collected data.

The initial scope includes 1) home automation and connected home products, and 2) wearable technologies, limited to health & fitness categories. It is envisioned that the framework will become the foundation criteria for a code of conduct and/or a certification program. Addressing the risks, the framework criteria have been organized into three sections: 1) Security, 2) User Access & Credentials and 3) Privacy, Disclosures & Transparency.

This framework does not override regulatory terminology, and as such, compliance with the framework and specification does not mean compliance with the law and/or regulations. The underlying recommendations are based on the Fair Information Practice Principles (FIPPs), building on security and privacy best practices advocated by the OTA, industry organizations and governmental agencies.[1, 2, 3, 4]

The framework represents rough consensus of the ITWG, reconciling input from nearly 100 organizations.[5] While members of the working group support the objectives of the framework, individual contributors and their respective organization may not support every criteria. The ITWG acknowledges technical limitations of devices with embedded firmware, and that some requirements today may not be applicable to every product, or feasible based on current design parameters, but should be the basis for future product development. While not central to the framework, the ITWG recommends the consideration of accessibility requirements to maximize access for users of all physical capabilities.[6] In addition, the working group recommends user administration controls in scenarios where multiple, identifiable individuals use the same devices and services.

Updates to this document and related resources will be posted at https://otalliance.org/IoT

[1] FIPPs are the widely accepted framework of defining principles to be used in the evaluation of programs that affect individual privacy. They are mirrored in the laws of many U.S. states, as well as 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

[5] Summary of public comments https://otalliance.org/iot-comments-draft-trust-framework

[6] See Web Accessibility Initiative: http://www.w3.org/WAI/; U.S. Accessibility requirements; Section 508 - https://en.wikipedia.org/wiki/Section_508_Amendment_to_the_Rehabilitation_Act_of_1973

IoT Trust Framework Pre-Release – Updated 11/24

IoT Trust Framework ● Required ○ Recommended N/A – Not Applicable	Connected Home	Wearable Tech
SECURITY		
1. Ensure devices support current generally accepted security transmission protocols.[7] All personally identifiable data in transit and in storage must be encrypted using current generally accepted security standards. [8,9] This is including but not limited to wired, WI-FI and Bluetooth connections.	●	●
2. All authentication credentials, including but not limited to passwords shall be salted and hashed and/or encrypted.[10, 11, 12]	●	●
3. All IoT support web sites must fully encrypt the user session. Current best practices include HTTPS or HTTP Strict Transport Security (HSTS) by default, also known as AOSSL or Always On SSL.[13, 14, 15]	●	●
4. IoT support sites must implement regular monitoring and continual improvement of site security and server configurations to acceptably reduce the impact of vulnerabilities.[16] Perform generally accepted 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 the research community. Remediate post product release design vulnerabilities and threats in a publically responsible manner either through remote updates and/or through actionable consumer notifications, or other effective mechanism(s).	●	●

[7] https://en.wikipedia.org/wiki/IPv6

[8] NIST Cryptographic Toolkit http://csrc.nist.gov/groups/ST/toolkit/index.html

[9] FTC Privacy & security in a Connected World - January 2015 Staff Report https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

[10] Limitations to Simple Hashing https://www.ftc.gov/news-events/blogs/techftc/2012/04/does-hashing-make-data-anonymous

[11] NIST Guide to Storage Encryption Technologies for End User Devices http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf

[12] NSA Suite B Cryptography is a set of cryptographic algorithms published by the National Security Agency. It serves as an interoperable cryptographic base for both unclassified information and most classified information. https://en.wikipedia.org/wiki/NSA_Suite_B_Cryptography

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

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

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

[16] See OTA Online Trust Audit https://otalliance.org/HonorRoll and recommended SSL test tools https://ota.ssllabs.com ; https://www.htbridge.com/ssl-check/

IoT Trust Framework ● Required ○ Recommended N/A – Not Applicable	**Connected Home**	**Wearable Tech**
6. All software and/or firmware updates, patches and revisions must either be signed and/or otherwise verified as coming from a trusted source.	●	●
7. Ensure all IoT devices and associated software, have been subjected to a rigorous software development lifecycle including unit, system, acceptance, regression testing and threat modeling.[17] Employ generally accepted code 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. For example for email communications must adopt SPF, DKIM and DMARC, for all security and privacy related communications and notices.[18]	●	●
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 for email to aid in securing communications and enhancing the privacy and integrity of the message.[19, 20]	○	○
USER ACCESS & CREDENTIALS		
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.*	●	●
12. Provide generally accepted recovery mechanisms for IoT application and support passwords and/or mechanisms for credential re-set using multi-factor verification (email and phone, etc.) where no user password exists.	●	●
13. Lock or disable user and device support account(s) after a reasonable number of invalid log in attempts. Companies may consider allow re-try *after a set period of time*, while preventing the ability of automated *logon attempts including but not limited to requiring use of CAPTCHA or similar mechanisms.*	●	●
14. Provide users notification of password reset or change utilizing secure authentication and /or out-of-band notice(s).	●	●

[17] See: https://www.sans.org/reading-room/whitepapers/analyst/integrating-security-development-pain-required-35060; Microsoft Secure Software Development Lifecycle (SDL) http://www.microsoft.com/en-us/sdl/default.aspx

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

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

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

IoT Trust Framework ● Required ○ Recommended N/A – Not Applicable	**Connected Home**	**Wearable Tech**
15. Enact a breach response and consumer notification plan to be reevaluated, tested and updated at least annually or after significant internal system, technical and/or operational changes. [21]	●	●
PRIVACY, DISCLOSURES & TRANSPARENCY		
16. Ensure privacy, security and support policies are easily discoverable, clear and readily available for review <u>prior</u> 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.[22]	●	●
17. Disclose the duration of *security support and patching*, (beyond product warranty). Such disclosures should map to the expected lifespan of the device.	●	●
18. Conspicuously disclose in its privacy policy how all personally identifiable and sensitive data types and attributes are collected and 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 period.	●	●
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 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 for product or service operation. *Require third party service providers are held to the same polices.*	●	●
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."	●	●

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

[22] Solutions may include providing a short notice on product packaging, point-of-sale materials as well as a link to an online privacy policy. 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 "read me first" packet affixed to the outside of the product box. It is recommended policies be designed utilizing a short-layered format. See http://www.truste.com/blog/2011/05/20/layered-policy-and-short-notice-design/ and http://privacynq.com/OTA as suggested examples.

IoT Trust Framework ● **Required** ○ **Recommended** **N/A – Not Applicable**	**Connected Home**	**Wearable Tech**
25. *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 provided.*[23]	●	●
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.	●	●
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 consumer value of opting in and sharing data be communicated to the end-user.*	●	●
28. Publically post the history of material privacy notice changes *for a minimum of two years.*	○	○
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 device or service data erasure and zeroization in the event of loss or sale.[24]	○	○

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." The inclusion of platforms is paramount as the IoT may be headed to a future where platform and OS providers and their respective connected ecosystems communicating on a seamless network may pose security and privacy risks.
2. It is expected that companies, products and services are in compliance with any law or regulation of the jurisdiction that governs the collection and handling of personal and sensitive information. Failure to do so constitutes non-compliance with this framework and results in automatic disqualification from any forthcoming code of conduct or certification program.
3. It is expected companies disclose details and terms of sharing information with law enforcement and reference any applicable transparency reports as legally permitted.
4. Smart devices refer to devices (and sensors) which are networked and may only have one-way communications.
5. Medical devices licensed and regulated by the FDA and/or prescribed by a physician are beyond the scope of the Framework, yet the majority of the criteria are deemed to be applicable.

[23] Parties should follow guidance that the Federal Trade Commission has established through legal actions and interventions.

[24] "Zeroization" https://en.wikipedia.org/wiki/Zeroisation