Online Trust Alliance

OTA Trust Framework Overview – Revised 10/15/2015

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 100,000's 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. The group recognizes "security and privacy by design" must be a priority from the onset of product development and be addressed holistically. The framework focuses on privacy, security and sustainability. The sustainability pillar is critical as it looks at the life-cycle issues related to long- term supportability and transfers of ownership of devices and the data collected.

The initial focus is on 1) home automation and connected home products, and 2) wearable technologies, limited to health & fitness categories. It is envisioned 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 a: 1) Security, 2) User access & credentials and 3) Privacy, Disclosures & Transparency.

The underlying 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 others.[2, 3, 4] The working group has attempted to incorporate global considerations and regulatory requirements. It is recognized existing and new regulations may supersede those outlined in the framework.

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 or may not support every criteria. The working group acknowledges there may be technical limitations of devices with embedded firmware, and that some requirements 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 working group recommends the consideration of accessibility requirements to maximize access for users of all ages and physical capabilities.[6] In addition, the working group recommends user administration controls in scenarios where multiple, identifiable individuals use the same devices and services.

The trust framework will evolve to reflect improving best practices, security standards, regulatory requirements and privacy principles. Updates 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

Online Trust Alliance

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. Smart devices refer to devices which are networked and may only have one-way communications.
3. Remove / Purge – Terms are used interchangeably to indicate the permanent deletion of users' identifiable and personal information.
4. Medical devices licensed and regulated by the FDA are out of scope, yet the majority of the criteria are deemed to be applicable.

IoT Trust Framework Pre-Release

IoT Trust Framework ● **Required** ○ **Recommended** **N/A – Not Applicable**	**Connected Home**	**Wearable Tech**
SECURITY		
1. Data Security – All personally identifiable IoT data in transit and in storage must be encrypted using current generally accepted security standards.[7],[8] This is including but not limited to wired, WI-FI and Bluetooth connections	●	●
2. PII Security – All sensitive and personally identifiable IoT information including passwords shall be hashed and or encrypted. [9, 10, 11]	●	●
3. Site Security – All IoT support web sites must fully encrypt the user session and adopt HTTPs by default, also referred to Always On SSL (AOSSL) wherever possible. [12, 13, 14]	●	●

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

[8] 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

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

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

[11] 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

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

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

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

IoT Trust Framework ● Required ○ Recommended N/A – Not Applicable	Connected Home	Wearable Tech
4. Server Security – IoT support sites must implement regular monitoring and continual improvement of site security and server configurations to acceptably reduce the impact of vulnerabilities. [15] Perform generally accepted penetration tests at least annually.	●	●
5. Email Security – IoT vendors using email communication must adopt email authentication protocols to help prevent spear phishing and maximize email deliverability by adopting generally accepted policies, such as SPF, DKIM and DMARC, for all consumer security and privacy related communications.[16]	●	●
6. Email Security – Within 90 days of publishing a DMARC policy implement a reject policy, helping ISPs and receiving networks to reject email which fail email authentication.	○	○
7. Email Security – 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.[17, 18]	○	○
8. Confirm no known critical vulnerabilities in software and hardware prior to release. Remediate post product release design vulnerabilities and threats in a publically responsible manner either through remote updates and / or through actionable consumer notifications.	●	●
9. Employ generally accepted code hardening techniques such as those to help prevent reverse-engineering, code tampering, and cryptographic key discovery.	○	○
10. All updates, patches and revisions of IoT application code must be cryptographically signed and verified from a trusted source.	○	○
11. Establish and maintain timely processes and systems to accept, track and respond to and third party vulnerabilities reports.	●	●
12. Insure all IoT devices and associated software, has been subjected to a rigorous software development lifecycle including unit, system, acceptance, regression testing and threat modeling.[19]	○	○
13. Ensure devices support current generally accepted security transmission protocols.[20]	○	○

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

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

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

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

[19] 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

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

USER ACCESS & CREDENTIALS		
14. For IoT user access, require first-use, system generated or one-time passwords; or alternatively use secure certificate credentials where no user password exists. As necessary, require separate and strong passwords for administrative access	●	●
15. 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.	●	●
16. Lock an IoT user or support account after a reasonable number of invalid log in attempts.	●	●
17. Ensure IoT password change availability following secure authentication and email or out-of-band notification of any password change.	●	●
18. Enact a breach response and consumer safety notification plan to be revised at least semi-annually and tested annually. [21]	○	○
19. Establish a user-friendly, responsive and secure mechanism for contacting the IoT vendor regarding product and service security risk issues.	●	●

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

IoT Trust Framework ● Required ○ Recommended N/A – Not Applicable		
PRIVACY, TRANSPARENCY & DISCLOSURES		
20. Ensure that privacy and security support policies of IoT vendors are clear and readily available for review prior to purchase, activation, download or enrollment and be easily discoverable and linked to their privacy policy. 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. In addition to prominent placement on their website, it is recommended companies utilize QR Codes, short URLs and other similar methods.[22]	●	●
21. Complies with global privacy regulatory requirements, such as COPPA, including indicating generally accepted opt-in/out clauses.	●	●
22. Require that changes to privacy policies be transparent and provide history of privacy notice changes.	○	○
23. Disclose the duration of product support (beyond product warranty). Such disclosures should map to the expected lifespan of the device.	●	●
24. Clearly and conspicuously disclose in its privacy policy how all personally identifiable and sensitive data types and attributes are collected and used. For example a fitness band would potentially disclose physical location, tracking and personal vitals (heart rate, pulse, blood pressure), as well as profile data.[23]	●	●
25. Disclose what functions will fail to function if connectivity becomes disabled or stopped. For home automation products, company must provide an alternative mechanism for access and use in the event of loss of connectivity (e.g., door openers, garage doors).	●	N/A
26. Disclose in its data retention policy that IoT data should be retained for as long as the user is using the device, or to meet legal requirements.	●	●

[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 https://consumer.privacynq.com/brief/b7809d19-53bc-4c6a-b22e-210cc94e7ee3 as examples.

[23] See FTC Guidance https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

IoT Trust Framework ● **Required** ○ **Recommended** **N/A – Not Applicable**		
27. IoT devices must provide a visible indicator and / or provide a user confirmation when initially pairing or connecting with other devices.	●	●
28. Provide the ability for the user or proxy to delete, or make anonymous personal or sensitive data (other than purchase transaction history) upon discontinuing, loss or sale of device.	○	○
29. Provide remote IoT device data erasure and zeroization in the event of loss or sale.[24]	○	○
30. Disclose in its privacy policy if and how IoT device/product/service ownership can be transferred (e.g., a connected home being sold to a new owner or sale of a fitness tracker.)	●	○
31. Only share consumers' personal data with third parties with consumers' affirmative consent, unless required for product or service operation.	●	●
32. Provide controls and/or documentation enabling the consumer to review and edit privacy preferences on the IoT device including the ability to reset to the "factory default."	●	●
33. Disclose commitment to not sell or transfer any 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.[25]	●	●
34. Adhere to the Fair Information Practice Principles (FIPPS) of minimal data collection.	●	●
35. Disclose details and terms of sharing information with law enforcement and reference any applicable transparency report.	●	●
36. If IoT data is stored in the cloud, adhere to generally accepted cloud security standards for IoT data.[26]	○	○
37. Disclose if personal and sensitive data, including but not limited to data which could reveal when a home may be occupied, is accessible. For example, does the thermostat collect the time of temperature changes and the location of or distance from the user (which could reveal when home is unoccupied)?	●	●
38. 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 on product packaging. The term (number of days) for product returns should be consistent with current exchange policies of the retailer, or specified in advance.	●	●

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

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

[26] https://cloudsecurityalliance.org/media/news/cloud-security-alliance-releases-new-guidance-for-identity-and-access-management-for-the-internet-of-things/