



IoT Trust Framework

Congressional Staff Briefing

November 19, 2015



Craig Spiegle
Executive Director & President

LEARN • INNOVATE • COLLABORATE

Who is OTA?

Mission to enhance online trust and empower users, while promoting innovation and the vitality of the internet.

- Goal 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.
- Collaborative public-private partnerships, benchmark reporting, meaningful self-regulation and data stewardship.
- U.S. based 501(c)(3) tax-exempt charitable organization.
- Global focus & charter.
- Supported by dues and donations.



LEARN • INNOVATE • COLLABORATE



Global Collaboration



LEARN • INNOVATE • COLLABORATE

IoT Working Group

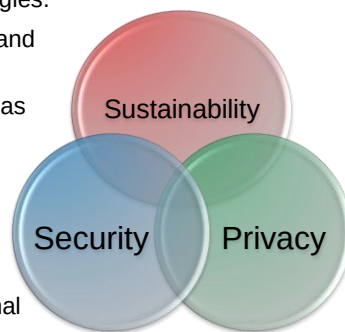
- Global Multi-Stakeholder Initiative
 - Formed in January 2015
 - Public & Private Sectors
- Scope
 - Connected Home & Wearable Technologies
 - Security, Privacy & Sustainability
 - Devices, Apps, Platforms and Cloud Services
- June - Face-To-Face Meetings & Weekly Calls
- Aug – Draft Released & Call for Public Comments
- Oct – Second draft released; heading towards last call
- Nov – Working group finalizing framework, code of conduct and foundation of certification program



LEARN • INNOVATE • COLLABORATE

Working Group Goals

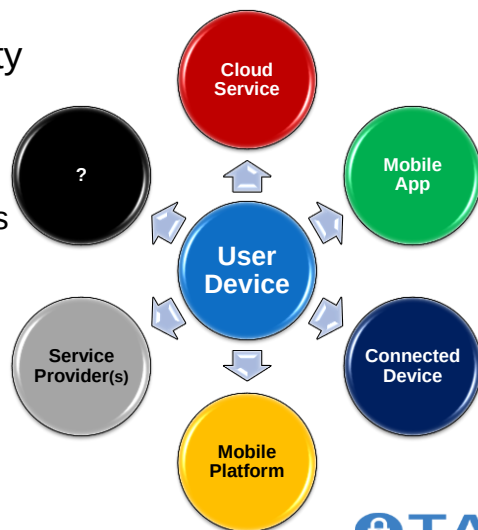
1. Focus on connected home & wearable technologies.
2. Provide guidance to help reduce vulnerabilities and adopt responsible privacy and data practices.
3. Drive the adoption of best practices; embracing as a voluntary, yet enforceable, code of conduct.
4. Provide recognition to companies, products and retailers who embrace the code of conduct.
5. Provide retailers / commerce sites criteria to aid in their product merchandising decisions.
6. Think globally; where possible, apply international standards and practices.
7. Encourage collaboration, sharing of best practices and threat intelligence.
8. Evaluate gating issues and considerations which may lead to the development of a seal or certification program.



LEARN • INNOVATE • COLLABORATE

Multi-Dimension Issues

- Device & Data Security
- Privacy
- Sustainability
 - Lifecycle considerations
 - Supportability
 - Data retention / ownership
- Data in use, transit & rest



LEARN • INNOVATE • COLLABORATE

The IoT Ecosystem

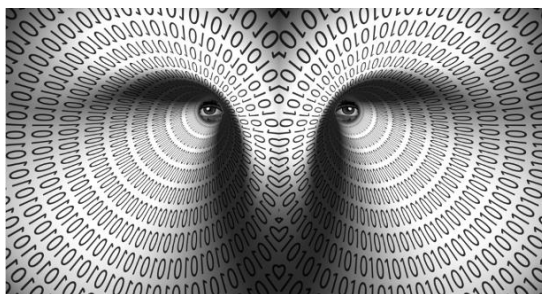
1. Highly personal, dynamic, persistent collection and transfer of data.
2. Reliance on a combination of devices, apps, platforms and cloud services.
3. Multiple data flows, touch points and disclosures.
4. Sustainability / lifecycle issues.
5. Lack of defined standards.
6. Non-traditional vendors



LEARN • INNOVATE • COLLABORATE

Ambient Data

- Growing number of devices & sensors
- Use & sharing with unknown or undisclosed third parties
- May be “benign” today, harmful tomorrow



LEARN • INNOVATE • COLLABORATE

The Smart Home

- Partnership with the National Association of Realtors
- Security, Privacy & Personal Safety
- Steps to “re-provision” your home
- Prior to occupancy, rental & at closing
- Prescriptive advice
- <https://otalliance.org/SmartHome>



LEARN • INNOVATE • COLLABORATE

Framework – Total of 30 Criteria

IoT Trust Framework ● Required ○ Recommended N/A – Not Applicable	Connected Home	Wearable Tech
SECURITY		
1. Data Security – 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. PII Security – All sensitive and personally identifiable information including passwords shall be hashed and or encrypted. ^{10, 11, 12}	●	●
3. Site Security – All IoT support web sites must fully encrypt the user session and adopt HTTPS or HTTP Strict Transport Security (HSTS) by default. (Also referred to as AQSSL or Always On SSL) ^{13, 14, 15}	●	●
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. ¹⁶ Perform generally accepted penetration tests at least annually.	●	●
5. Establish and maintain timely processes and systems to accept, track and respond to external vulnerabilities reports. Remediate post product release design vulnerabilities and threats in a publicly responsible manner either through remote updates and / or through actionable consumer notifications.	●	●
6. All software updates, patches and revisions must be signed and/or verified 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 such as those to help prevent reverse-engineering, code tampering, and cryptographic key discovery.	●	●
8. 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. ¹⁸	●	●
9. Email Security – Within 180 days of publishing a DMARC policy implement a reject policy, helping ISPs and receiving networks to reject email which fail email authentication.	○	○
10. 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. ^{19, 20}	○	○



LEARN • INNOVATE • COLLABORATE

User Access & Credentials

USER ACCESS & CREDENTIALS		
11. For user access, require first-use, system generated or one-time passwords; or alternatively use secure certificate credentials. As necessary, require unique passwords for administrative access.	●	●
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 user or support account(s) after a reasonable number of invalid log in attempts.	●	●
14. Provide users notification of password reset or change utilizing secure authentication and /or out-of-band notifications.	●	●
15. Enact a breach response and consumer notification plan to be reevaluated and updated to incorporate internal system, technical and operational changes. ²¹	●	●



LEARN • INNOVATE • COLLABORATE

Privacy, Transparency & Disclosures

PRIVACY, TRANSPARENCY & DISCLOSURES		
16. Ensure privacy and security support practices are easily discoverable, clear and readily available for review prior to purchase, activation, download or enrollment. In addition to prominent placement on their website, it is recommended companies utilize QR Codes, short URLs and other similar methods. ²²	●	●
17. Disclose the duration of product support (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 purpose for which it is being collected in accordance with the privacy policy.	●	●
19. Disclose what features 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
20. 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.	●	●
21. IoT devices must provide a visible indicator and / or provide a user confirmation when initially pairing or connecting with other devices.	●	●
22. 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.)	●	○
23. Only share consumers' personal data with third parties with consumers' affirmative consent, unless required for product or service operation and parties hold such data in confidence.	●	●
24. 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."	●	●
25. 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. ²³	●	●



LEARN • INNOVATE • COLLABORATE

Privacy, Transparency & Disclosures

IoT Trust Framework	● Required	○ Recommended	N/A – Not Applicable	Connected Home	Wearable Tech
25. 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. 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 on product packaging. The term (number of days) for product returns shall be consistent with current exchange policies of the retailer, or specified in advance. (Under review)	●			●	●
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.	●			●	●
28. Require that changes to privacy policies be transparent and publically post the history of privacy notice changes.	○			○	○
29. 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.	○			○	○
30. Provide remote IoT device data erasure and zeroization in the event of loss or sale. ²⁴	○			○	○



LEARN • INNOVATE • COLLABORATE

What's Next?

- Reconcile feedback from November IoT Summit
- Develop an implementation guide
- Drive a proof of concept “pilot”
- Expand collaboration with other organizations.
- Engage retailers and online merchants
- Secure funding & grants for pilot projects
- Recognize early adopters who embrace code / pledge.
- Develop incentives
- Develop criteria as the basis for a certification program.



LEARN • INNOVATE • COLLABORATE

More Information

IoT Initiative <https://otalliance.org/IoT>

Smart Home <https://otalliance.org/SmartHome>

Presidential Candidate Audit
<https://otalliance.org/2016Candidates>

Craig Spiegle

craigs@otalliance.org

+1-425-455-7400



LEARN • INNOVATE • COLLABORATE