

IoT Trust Framework

leading to self regulation code of conduct and certification models


Craig Spiegle
Executive Director & President
Online Trust Alliance

LEARN · INNOVATE · COLLABORATE

Who is OTA?

Mission to enhance online trust and empowering 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



Focused on Collaboration



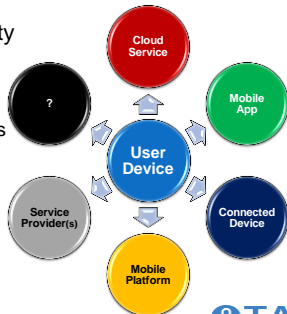
The IoT Ecosystem

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 market players.



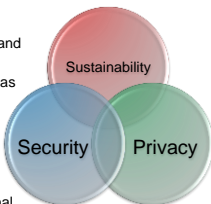
Multi-Dimension Issues

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



Working Group Goals

1. Phase 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

Framework Excerpts - Sustainability

- Disclose what functions will work if "smart" functions are disabled or stopped
- Provide a mechanism for transfer of ownership including providing updates for consumer notices and access to documentation/support
- Publish a timeframe for support after a device/app is discontinued or replaced by a newer version



LEARN · INNOVATE · COLLABORATE

Where We Are

- January – Working Group Formed
- June – Working draft of principles & goals ratified
- Aug – Public draft released with call for comments
- Sept – Over 100 comments received
- October 19 – 2nd public draft released (today)
- November 18
 - Last call
 - Face-to-Face IoT Trust Summit in Washington DC.



LEARN · INNOVATE · COLLABORATE

Framework – Total of 38 Criteria

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. ¹⁷ This is including but not limited to wired, Wi-Fi and Bluetooth connections	●	●
2. PIN Security – All sensitive and personally identifiable [IoT] information including passwords shall be hashed and/or encrypted. ^{18, 19, 21}	●	●
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, 24}	●	●
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. ¹⁹ 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 mitigate email deliverability by adopting generally accepted policies, such as SPF, DKIM and DMARC, for all customer security and privacy related communications. ¹⁸	●	●
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.	○	○

iTA
Online Trust Alliance

LEARN · INNOVATE · COLLABORATE

User Access & Credentials

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.	●	●

iTA
Online Trust Alliance

LEARN · INNOVATE · COLLABORATE

Privacy, Transparency & Disclosures

IoT Trust Framework ● Required ○ Recommended N/A - Not Applicable

	Connected Home	Wearable Tech
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/opt-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 opener, garage door).	●	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.	●	●

iTA
Online Trust Alliance

LEARN · INNOVATE · COLLABORATE

What's Next?

- November 18 - IoT Trust Summit, Washington DC.
<https://otalliance.org/news-events/upcoming-events>
- Consolidate feedback, release initial framework.
- Validate global considerations.
- Pursue a voluntary code of conduct (some companies already using it as vendor "checklist"), evolving to an enforceable code of conduct.
- Develop criteria as basis for a certification program.
- Expand collaboration with other organizations.



LEARN · INNOVATE · COLLABORATE

More Information

- Submit Comments – We will review all!
<https://otalliance.org/iot-trust-framework-submission>
- Join the working group
https://otalliance.org/system/files/files/member/documents/ota_iot_membership_application-2015v2.pdf
- Working group meeting in Washington, D.C. – November 18
<https://otalliance.org/news-events/upcoming-events>
- Contact us for more info:
<https://otalliance.org/lot> +1-425-455-7400



LEARN · INNOVATE · COLLABORATE
