Online Trust Alliance

IoT Trust Framework

leading to self regulation, codes of conduct and certification models

Craig Spiezle
Executive Director & President
Online Trust Alliance
craigs@otalliance.org
October 6, 2015

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 over 100 organizations including retailers, commerce sites, interactive marketers, members of the advertising ecosystem and technology providers.

Online Trust Alliance

LEARN • INNOVATE • COLLABORATE

Focused on Collaboration

LEARN • INNOVATE • COLLABORATE

The Consumer IoT Ecosystem

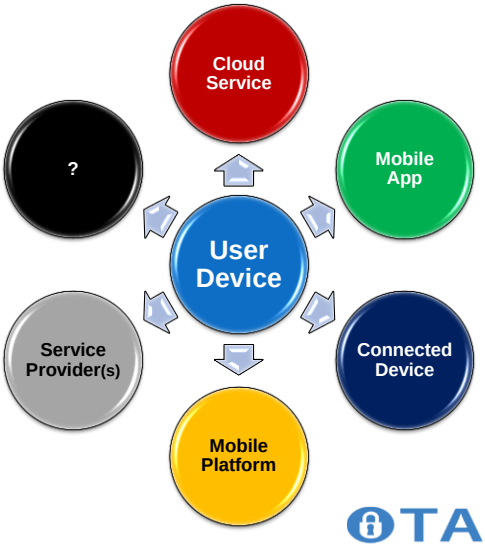
1. Highly personal, dynamic, persistent collection and transfer of data.
2. Reliance on a combination of devices, apps, platforms and cloud services.
3. Multiple data flows.
4. Multiple touch points and disclosures.
5. Sustainability / lifecycle issues.
6. Lack of defined standards.
7. Non-traditional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

Online Trust Alliance

LEARN • INNOVATE • COLLABORATE

Multi-Dimension Issues

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

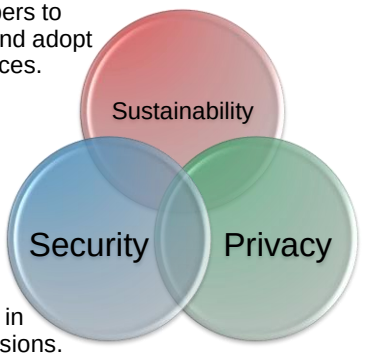


OTA Online Trust Alliance

LEARN • INNOVATE • COLLABORATE

Working Group Goals

1. Provide guidance to manufacturers and developers to help reduce attack surface and vulnerabilities, and adopt responsible privacy and data stewardship practices.
2. Drive the adoption of best practices; embracing "privacy and security by design", as a model for the development of a voluntary, yet enforceable code of conduct.
3. Provide positive affirmation and recognition to companies, products, and retailers who embrace the code of conduct and meet minimum standards.
4. Provide retailers / commerce sites criteria to aid in their product merchandising and promotion decisions.
5. Where possible, apply existing standards from NIST, NTIA, ISO and other industry working groups.
6. Encourage collaboration, sharing of best practices and threat intelligence.
7. Evaluate and identify gating issues and considerations which may lead to the development of a seal or certification program which could become an incentive to adopt best practices.



OTA Online Trust Alliance

LEARN • INNOVATE • COLLABORATE

Sample Framework Elements

Security

- Prompt/change default passwords
- Encrypt data in motion and at rest
- Remediate vulnerabilities remotely or by notifying customers
- Sign/verify all updates/patches/ revisions

- Privacy policy must be easily available before purchase, disclose consequences of opt out re: product features
- Disclose personally identifiable data types and attributes collected
- Data sharing only with third parties who agree to confidentiality, use for specific purpose

Sustainability

- Disclose what functions work if “smart” disabled
- Disclose whether user can remove/purge personal or sensitive data upon loss, damage, sale, end of life
- Provide mechanism for transferring ownership of devices/services

OTA Online Trust Alliance

LEARN • INNOVATE • COLLABORATE

IoT Trust Framework – Aug Draft

- Developed collaboratively in the IoT Working Group, released Aug 11th
- Addresses security, privacy, sustainability issues
- High-level, not calling out specific protocols, etc.
- 23 “must have’s”, 12 “should have’s”
- Call for public comment, deadline was September 21

OTA Online Trust Alliance

LEARN • INNOVATE • COLLABORATE

Request for Comments

- Deadline was September 21, but will review others times permitting.
- Approximately 100 public and private comments submitted to-date.
- In process of being reconciled and clarified
- Expanding to approximately 50 principles and criteria

OTA Online Trust Alliance

LEARN • INNOVATE • COLLABORATE

Security – Draft

SECURITY		
1. Data Security – All personally identifiable data in transit and in storage must be encrypted using current NIST and industry recommendations applicable to their application and industry.[1]	●	●
2. PII Security – All sensitive and personally identifiable information including passwords shall be hashed and or encrypted. [2, 3]	●	●
3. Site Security – All web sites must fully encrypt the user session and adopt HTTPs by default, also referred to Always On SSL (AOSSL) where ever possible. [4, 5, 6]	●	●
4. Server Security – Sites must implement monitoring of site security and server configurations using testing tools no less than monthly and help identify and remediate any vulnerabilities. [7]		
5. Email Security – Sites must adopt email authentication protocols to help prevent spear phishing and maximize email deliverability by adopting SPF, DKIM and DMARC policy for all consumer security and privacy related communications.[8]	●	●
6. Email Security - Publish a reject DMARC policy, helping ISPs and receiving networks to reject email which fail email authentication.	o	o
7. Email Security – Adopt transport-level confidentiality including STARTTLS and opportunistic Transport Layered Security (TLS) for email to aid in securing communications and enhancing the privacy and integrity of the message.[9, 10]	o	o

OTA Online Trust Alliance

LEARN • INNOVATE • COLLABORATE

Disclosures & Privacy

DISCLOSURES & PRIVACY		
20. The privacy and security support policies must be readily available for review prior to consumer purchase, activation or enrollment and be easily discoverable to the user including a link to the privacy policy displayed in a way readily accessible to consumers. 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. In addition to prominent placement on their website, is recommended companies utilize Q Codes, short URLs and other similar methods.13	●	●
21. The privacy policy should be made available in languages other than English	o	o
22. Changed to privacy policies should be transparent and provide a history of privacy notice changes	●	●
23. Disclose the duration of product support (being product warranty). Such policies should map to the expected lifespan of the device.	●	●
24. Clearly and conspicuously disclose all personally identifiable data types and attributes collected and how such data will be used. 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.	●	●
25. Disclose what functions will stop working if connectivity or "smart" capability becomes disabled or stopped. 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).	●	N/A
26. Disclose the term and duration of the data retention policy. Data should be retained for as long as the user is using the device, or to meet legal requirements.	●	●
27. Device must provide a visible indicator and user confirmation when paring or connecting with other devices.	●	●
28. Provide the ability to delete all data upon account termination or user request. The user should have the ability to remove, or make anonymous personal or sensitive data (other than purchase transaction history) upon discontinuing device use, loss or sale of device.	o	o
29. Provide remote device wiping in the event of loss or sale.	o	o

Online Trust Alliance

User Access & Credentials

USER ACCESS & CREDENTIALS		
15. Use default passwords which prompt for reset or change on first use or are uniquely; use secure certificate credentials where no user password exists. As applicable, separate passwords should be required for administrative access.	●	●
16. Provide secure recovery mechanisms for passwords and/or provide mechanism for credential re-set where no user password exists. Suggestions include multi-factor verification (email and phone, etc.) as well as incorporate lockout capability for multiple sign-on attempts.	●	●
17. All updates, patches and revisions must be cryptographically signed and verified. Such signing helps to insure the integrity of the patch and to verify the proper developer.	o	o
18. Establish and review at a minimum semi-annually a breach response and consumer safety notification plan. Recommended best practices including conducting employee training programs and "tabletop" or breach simulation exercises. [12]	o	o
19. Establish and maintain timely and secure mechanisms for users to contact the company regarding issues, including but not limited to the loss of the device, device malfunction, account compromise, etc.	●	●

Online Trust Alliance

Open Questions

1. Consider a rating or scoring scale for certification.
2. Will all criterial be weighed the same?
3. Need to define who would be subject to the requirements? Device mfgs, platform providers, the entire ecosystem?
4. Considerations for data/network isolation?
5. What about meta data?
6. Concerns about devices with limited power (battery and chip)
7. Requirement may to taxing, dramatic and potentially very costly
8. Multi-user environments (family)
9. Data collection of minors
10. Should source code be made public?

OTA Online Trust Alliance

LEARN • INNOVATE • COLLABORATE

What's Next?

- Consolidate feedback, release initial framework November 18.
- Review 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.

OTA Online Trust Alliance

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/Iot +1-425-455-4500

OTA
Online Trust Alliance

LEARN • INNOVATE • COLLABORATE