Comments on the Online Trust Alliance's Proposed Internet of Things Best Practices Framework

September 14, 2015

Recently, the Online Trust Alliance (OTA) published a request for comments on their Internet of Things (IoT) trust framework. The framework serves as a set of best practices for companies creating products in the IoT environment.

The framework lays out 23 "proposed minimum requirements" as well as 12 "additional recommendations" - additional practices companies who want to go beyond the bare minimum might want to engage in. We divide our comments here into two sections to mirror this structure, one devoted to the proposed minimum requirements, and one dedicated to the proposed additional (non-mandatory) requirements.

Feedback on the Proposed Minimum Requirements

Overall, the minimum requirements are thoughtful and principled . CDT has no major changes - most of our feedback centers around adjusting wording to make sure edge cases are covered, which we enumerate below.

We believe that requirement 2, which recommends optimizing consent screens for readability, should also address accessibility. For example, the section suggests that in some cases devices will be so minimal as to *"requir[e] the user to review and consent using another device"*. This is well intentioned in terms of readability, but could be problematic for some users. Any solution requiring a second device is exclusive and we believe this framework should apply to a broad section of IoT users, including those who do not own multiple devices as well as those with devices without any display whatsoever. To achieve stronger inclusivity and flexibility, requirement 2 should read : "requiring the user to review and consent

using another device **or format."** Examples of this might include a printed copy of the consent notice included with the instruction manual for a . Additionally, we believe requirement 2 should strongly suggest that any consent notice be placed conspicuously on the manufacturer's website as well as displayed when creating user accounts on the device so that future owners of the IoT product, who may not have the original packaging materials, can also make an informed decision.[1]

In minimum requirement 4, there is a typo: "including tan explanation" should read "including an explanation."

For minimum requirement 5, it is unclear what the difference is between "term" and "duration" of data retention. It appears that "term" refers to the conditions under which data is collected and duration is the time after which collected data is no longer retained, but this should be clarified.

For minimum requirement 7, more detail is needed on the subject of hashing and encryption. First, unless a random salt is added to the hash, small inputs such as IP addresses, MAC addresses, SSNs, etc. can be easily brute forced (meaning all combinations can be tried as fast as possible). During his tenure at the Federal Trade Commission as Chief Technologist, Ed Felten prepared a useful primer on why simple hashing does not always anonymize data.[2] In addition, OTA may want to point to resources for companies to determine best practices for encryption, such as NIST's "Guide to Storage Encryption Technologies for End User Devices."[3]

---

[1] Another promising idea may be to physically embed, etch, print, etc. the website for the device/service on the physical good itself, but this obviously must be flexible.
[2] Does Hashing Make Data "Anonymous"?
https://www.ftc.gov/news-events/blogs/techftc/2012/04/does-hashing-make-data-anonymous
[3] NIST Special Publication 800-111: Guide to Storage Encryption Technologies for End User Devices
http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf

Minimum requirement 11 mandates that manufacturers conduct penetration testing. While other requirements in the framework point to minimum standards currently used in industry, this requirement does not refer to any appropriate penetration testing standards or methodologies. We recommend that OTA refer manufacturers to formalized penetration testing methodologies such as the Penetration Testing Execution Standard (PTES.)[4].

For minimum requirement 12, which suggests that "upgradability capabilities be clarified to the consumer in advance of purchase", we would recommend including required language that manufacturers must use in a product's packaging. We would also recommend the framework task industry with creating an agreed-upon icon that signifies to consumers whether or not a device can be updated. Any such icon should be placed prominently, to supplement any textual warnings so that consumers can easily recognize an IoT device that will receive updates compared to those that will not.

Minimum requirement 16 should state explicitly that signing and verification should be *cryptographic* signing and *cryptographic* verification. The language can be easily changed to: *"All updates, patches, revisions, etc. must be* ***cryptographically*** *signed/verified..."* Ideally, the requirements would point to minimum accepted ciphers and signature schemes, but we are unaware of any IoT-specific guidance in this area that balances the resource constraints of embedded devices against common IoT threat models.

Minimum requirement 22 helpfully requires manufacturers to specify what functionality is available if "smart" functions are disabled or rendered unavailable. However, it is unclear what makes a function "smart." If this term only applies to networking the device, then the word "smart" should be changed throughout to

[4] http://www.pentest-standard.org/index.php/Main_Page

simply "networked." If "smart" applies to other types of functionality – for example, a particular patented functionality or a "big data functionality" that doesn't intrinsically depend on network access then other descriptive words should be used.

CDT would recommend adding "transport-level confidentiality" to requirement 23's bolded text. This would serve to emphasize that while authenticated email is one aspect of confidentiality, transport-level confidentiality support, when available, is considered a best practice as well.

Feedback on Additional Requirements

Overall, the additional requirements look reasonable. We include some feedback on these additional elements below.

Additional requirement 1 states companies should commit not to transfer consumer data should not be part sold during bankruptcy unless required for product functionality. This principle is of paramount importance, since new owners may have very different privacy practices. Therefore, we recommend this requirement be moved into the proposed minimum requirements.

Additional requirement 4 would require manufacturers to disclose if personal data is stored and accessed in the cloud, but it invites ambiguity. For example, a connected thermostat storing time and temperature changes in the cloud isn't clearly storing personal data. We recommend adding language such as: "which could reveal when during the day a home is unoccupied" to the end of the example.

Additional requirement 6 states *"Provide history of privacy notice changes available for review and or comparison..."* Changes to privacy policies should be transparent

and part of that transparency means allowing users to compare their new privacy with the previous. We recommend this requirement be incorporated into the minimum requirement list instead of additional requirements.

For further information please contact:

- Staff Technologist, Greg Norcie (norcie@cdt.org)
- Chief Technologist, Joseph Lorenzo Hall (joe@cdt.org)