To: Online Trust Alliance, Bellevue, WA

From: Josh Datko, Founder, Cryptotronix, LLC

Subject: Comments on the IoT Trust Framework Draft, Dated 13 August 2015

Date: September 19, 2015

---

1 General Comments

1. It's not clear how this framework becomes a certification process. Does a manufacturer submit an application with a statement saying that they met the requirements? Does a third-party have to perform the assessment? What is the cost of the certification and for how long is it valid? Is the certification per product SKU or for a family of products?

2. I recommend you consider a scale, perhaps numeric or grading-system where manufacturers receive some credit and recognition. Companies that complete all or most of the requirements would receive an A+ for example, which might give companies that only have received a B, an incentive to complete the remaining items. Additionally, this grading scale may help adoption as some companies may already qualify for a B rating (whatever that is), which helps build momentum for further adoption and refinement.

3. Echoing other reviewers, consider having several *profiles* of the specification. Some devices may not have any user password, therefore the password requirements would not apply. Can a certification applicant mark a requirement *Not Applicable*? Continuing with the score-based-approach recommendation, instead of a minimum number of requirements, perhaps a score of weighted ones. Otherwise it may be challenging to draft a set of requirements that apply equally to the heterogeneous IoT field.

4. Technical requirements should provide a clear reference to a published specification like an IETF RFC, NIST SP, OASIS Standard, etc... This provides clearer guidance to implementers and makes this framework easier to verify. Instead of the phrase "best practices", specify a list of acceptable standards. The list can be an appendix as it would probably change faster then the requirements.

5. Further echoing other reviewers, companies should be required to publish a responsible disclosure policy for reporting security vulnerabilities.

2 Comments on Proposed Minimum Requirements

The number of each comment in the following section corresponds to listed number requirement in the draft.

1. Consider adding the requirement that the changes between privacy policies be publicly available. At minimum, the previous privacy policies documents must remain available but companies should highlight changes between revisions.

2. Reading anything on a smart-phone is a horrible experience, especially a privacy policy. Instead of optimizing for readability on the user's interface just instead optimize for readability in general. An example is SparkFun Electronics Terms of Service[1]; the *legalese* is placed side-by-side with human understandable translations.

4. I recommend that this item carry additional requirements. Specifically, consider including the requirement that all third-party data services must be clearly identified regardless of the purpose. This requirement should also specify the exact data being shared. Also, I'm not sure the company-under-certification can do anything besides accept at face value what the third party claims. I rather see companies be upfront about why and what they are sharing, with the intent of having them share less data, then to share more data with third parties. The more third-party sharing, the greater potential for compromise of user data.

6. The words *remove*, *purge*, and *made anonymous* should be further defined. Does remove mean that the show-to-the-user flag is cleared? Does purge mean the data is no longer in the database or no longer in one database. The question, of importance to users, is *does the company still have access to this data after I delete/purge it*?

16. This requirement is too vague to produce a verifiable implementation. For example, if a manufacturer hashes a revision with MD5 and provides the revision plus the hash as the verification, would that meet this requirement? It would seem like it would but I'm not sure that's the intent of this requirement. Referring to a published specification would help here.

22. *Connectivity* should be clarified as the connection between a home-automation device and a cloud-based server. A garage door opener needs to be connected to the receiver for it to work, however it only needs to be connected to the cloud for the remote open feature. I think the device-cloud connections should be focus of this requirement.

3 Comments on Additional Recommendations

1. I don't think there is a proper incentive for companies to adopt these additional recommendations. These should be incorporated into the framework or there should be a mechanism that allows an applicant to receive recognition for these additional measures.

2. In general, these items seem less refined and more vague then the requirements in the *Proposed Minimum Requirements* section.

Josh Datko

[1] `https://www.sparkfun.com/terms`