September 10, 2015

ICRT International Consumer Research & Testing

24 Highbury Crescent | London N5 1RX | UK | Tel: + 44 (0) 207 563 9170 | Fax: +44 (0) 207 563 9171

Dear Mr. Spiezle.

As comments are invited before 14 September our ICRT Working Group would like to submit some comments, please refer to annex. I hope you will consider these comments for adoption. We are certainly interested to know what the status of the Framework will be after finalization and how it will be used or distributed. I want to state clearly that ICRT as an independent consumer organization and not being a member of OTA, does not endorse the Framework document.

However we are prepared to discuss possible future cooperation

Kindest regards,

Harke Smits
ICRT/Test Achats

Comments by ICRT in color.

PROPOSED MINIMUM REQUIREMENTS – IoT TRUST FRAMEWORK

The following requirements are the proposed baseline for any self-regulatory and/or certification program. It should be noted in addition to what is outlined below, companies must adhere to all regulatory requirements as they pertain to where their users or consumers reside, including but not limited to breach notification, disclosure requirements, child protection, anti-spam and related consumer protection laws and regulations.

1. The privacy policy must be readily available to review prior to product purchase, download or activation and be easily discoverable to the user and easily to understand. 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. Solution may include a short notice on product packaging, user guide, point-of-sale materials as well as a link to online privacy policy. It is recommended a link to the privacy policy be on the header and/or footer of every web page including product registration page and application download page. The working group acknowledges the need to have flexibility in how and when notices are provided. In some cases notices may be provided on first use or when activating a new feature or within the welcome information packet included with physical product.

2. The privacy policy display must be optimized for the user interface to maximize readability. The working group recommends all policies be designed utilizing a short-layered format and recognizes the

user interface may be limited for readability, requiring the user to review and consent using another device.5

3. Manufacturers must conspicuously disclose all "personally identifiable" (could we have a definition of this term?) data types and attributes collected. 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. All privacy setting options should be defaulted to 'opt in' to provide consumers with a greater level of protection

4. Any default personal data sharing must be limited to third parties/service providers who agree to confidentiality and to limit usage for clearly specified purposes. Acceptable usage would be limited to support product features and functionality; product improvement; or delivery of services on behalf of the application developer or manufacturer. Any sharing of personal data with third parties for other purposes must be disclosed and require opt-in, including ~~t~~an explanation of the nature and scope of the data shared and limitations on the use of the data if any. This requirement places the responsibility on the manufacturer to manage their third party service providers to comply. Does this come within the scope of the EU Safe Harbor Principles?

5. The term and duration of the data retention policy must be disclosed. In general, data should be retained for as long as the user is using the device, or to meet legal requirements. It is acceptable for the policy to state data will be retained as long as a customer uses the product or service, implying that it ~~and must~~ will be deleted from all data storage locations (including those of any third parties) upon expiration or account termination.

6. Manufacturers must disclose if (and how) the user has the ability to remove, have purged or made anonymous personal and sensitive data (other than purchase transaction history) upon discontinuing device use, loss, damage, sale or device end-of-life. The working group believes this capability should be provided at no-charge.

7. Personally identifiable data must be encrypted or hashed at rest (storage) and in motion using best practices including connectivity to mobile devices, applications and the cloud utilizing Wi-Fi, Bluetooth, cellular data and any other communication methods. As a best practice the goal is to achieve end-to-end encryption of all personal data. Note this would not apply to direct wired connections of the device. This requirement requires the use of ~~current~~ encryption technologies ~~solutions~~ currently being deployed by industry that are considered uncompromised by available techniques.

8. Default passwords must be prompted to be reset or changed on first use or uniquely generated "complex" passwords. Where possible, separate passwords should be required for administrative vs user access and not permit password reuse. Ideally passwords should be randomly generated.

9. All user sites must adhere to SSL best practices using industry standard testing mechanisms. For example the working group suggests sites score a minimum of 90% using industry benchmark testing tools.6

10. All device sites and cloud services must utilize HTTPS encryption by default, ~~-~~ a~~A~~lso referred to as HTTPS everywhere or Always On SSL (AOSSL). Recognizing the importance of HTTPS, Google has issued an advisory for all consumer ~~-~~facing websites and the White House has mandated that all U.S. government agencies implemented it by December 31, 2016.7, 8, 9

11. Manufacturers must conduct penetration testing for devices, applications and services. The objective is to help identify and patch vulnerabilities. Ideally such testing should be independently verifiable.

12. Manufacturers must have capabilities to remediate vulnerabilities in a prompt and reliable manner either through remote updates and / or through consumer notifications and concise, easy-to-carry-out instructions. Alternatives could be device replacement or manufacturer upgrade, product recall or onsite service for connected home devices. It is recognized some embedded devices' current design may not have this capability and it is recommended such update / upgradability capabilities be clarified to the consumer in advance of purchase, and an option to disable online capability provided.

13. Manufacturers must have a breach response and consumer safety notification plan, at a minimum reviewed semi-annually. Recommended best practices including conducting employee training programs and "tabletop" or breach simulation exercises.10

14. Manufacturers must provide secure recovery mechanisms for passwords. Suggestions include multi-factor verification (email and phone, etc.) as well as incorporate lockout capability for multiple sign-on attempts.

15. Device must ~~provide a visible indicator or~~ require user confirmation when initially pairing or connecting with other devices and~~.~~ provide a visible indicator when paired.

16. All updates, patches, revisions, etc. must be signed/verified. Such signing helps to insure the integrity of the patch and to verify the source or developer.

17. For products and services which are designed to be used by multiple family members and collect each user's PII, manufacturers need to incorporate the capability for creating individual profiles and/or have parental or administrative level controls and passwords.

18. Manufacturers must publish and provide timely mechanisms for users to contact the company regarding issues including but not limited to the loss of the device, device malfunction, account compromise, etc.

19. Manufacturers must provide a mechanism for the transfer of ownership including providing updates for consumer notices and access to documentation and support.11

20. The device must have controls and/or documentation enabling the consumer to set, revise and manage privacy and security preferences including what information is transmitted via the device. Passwords must be able to be changed by the user at any time, following secure authentication, and a notification of any password change must be transmitted to the user. Capabilities should include ability to reset to the "factory default."

21. Manufacturers must publish to consumers a time-frame for support after device/app is discontinued or replaced by newer version. This is recommended beyond traditional warranty policies and should be for the life of the device.

22. Manufacturers must disclose what functions will fail to work if "smart" functions are disabled or stopped. Core functions must remain operative in the event the smart component is disabled. 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).

23. ~~Configure~~ Aall security and privacy related email communications ~~to~~ must adopt email authentication protocols. Current standards include SPF, DKIM and DMARC which aid in the ability counter email fraud, malicious emails and spear phishing exploits.12 Additionally, organizations and manufacturers should consider STARTTLS and opportunistic Transport Layered Security (TLS) for embedded email functions to aid in securing communications and enhancing the privacy and integrity of the message.13, 14

ADDITIONAL RECOMMENDATIONS

The following is a preliminary list of recommendations and considerations organizations and manufacturers may wish to consider above and beyond those outlined in the framework. It is recognized that some of the following may be not be applicable to every device or service.

1. Make a commitment to not transfer any consumer data unless it is a dependent part of the sale or liquidation of the core business which originally collected the data, or unless company has taken reasonable steps to provide consumer notice and consent to such transfer (with the exception of data required to perform product support and functionality as specified in the original product terms of use and privacy policy).

2. Take steps to help prevent personal data from being re-identified. [need definition here]

3. Adhere to the Fair Information Practice Principle of minimal data collection.

4. Disclose if personal data is being stored and accessed in the cloud. For example does the manufacture of a connected thermostat collect the time of temperature changes or the location of or distance from the user?

5. Agree to not materially change privacy policies after the product is purchased without consumer consent, providing the core product functionality is not impacted.

6. Provide history of privacy notice changes available for review and or comparison.15

7. Plan for the need to include support for evolving protocols/standards.

8. As applicable, require third-party installers be trained to configure devices per security and privacy best practices such as usage of randomly generated usernames and passwords.

9. Provide the ability for a consumer to return a product without charge after reviewing the privacy practices that are presented during initial set up. Such policies should be consistent with current exchange policies of the retailer and or industry. Note: This is a great consumer centric recommendation that would be good to get into the minimum requirements section.

10. Disclose if the personal data is portable and compatible to common technical standards in a non-proprietary format.

11. Provide configuration roll-back capability in the event a non-security related upgrade conflicts with other connected devices.

12. Manufacturers should optimize the device interface and usability for users with vision, hearing and mobility limitations to maximize use and access for users of all ages and physical capabilities.