Comments on OTA Draft IoT Trust Framework
Submitted 9/22 (Author: Anonymous; Industry: Internet of Things)

Item #1 **–**

> **The privacy policy must be readily available to review prior to product purchase, download or activation and be easily discoverable to the user. 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, 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 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.

Edit text to: "… The solution may include a short notice on product packaging, point-of-sale materials as well as a link to a privacy policy posted online. It is recommended a link to the privacy policy be displayed in a way that makes it readily accessible to consumers."

Item #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.

Disagree with [suggested] addition to have previous policies available for comparison. Material changes already require consent mechanism. Lets focus on the Item itself.

Item #3 –

> **Manufacturers must conspicuously disclose all personally identifiable 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.

Edit text to: "**Manufacturers must conspicuously disclose categories of all personally identifiable data types and attributes collected."** …

Agree as edited provided it is understood this is about data types and does not require a drill down into specific field level transparency.

Item #4 –

> **Any default personal data sharing must be limited to third parties/service providers who agree to confidentiality and to limit usage for 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 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.

Edit text to: "…product improvement; delivery of services on behalf of the application developer or manufacturer; or sharing that is contemplated, or inherent in, the functionality of the device."…

Do not support the suggestion [by another group] to publish specific vendors and their contact information.

Item #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 and must be deleted upon expiration or account termination.

The intent of this statement is captured in the first sentence of [this] guideline. The second sentence in guideline beginning with "It is acceptable…" should be deleted as it could be treated as some type of new standard. There may be valid business and legal reasons to retain data past account termination date.

Item #6 –

> **Manufacturers must disclose if 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.

Edit text to: "**Manufacturers should consider what rights the user has 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."** Delete non-bolded statement.

Aspirational requirement needing further development to differentiate between existing equipment and newly designed equipment; possible in the "green field" of innovation but so difficult to implement in exiting equipment that consensus from established OEMs on existing equipment will be very difficult to reach.

Item #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 and 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.

Everything <u>not</u> in bold should be deleted. It is overly broad and likely unachievable.

Should be rewritten. Preferred route is to frame the guideline in terms of "providing transparency around encryption practices and then letting the consumer decide".

If it is retained in some format, would like rationale for "would not apply to direct wired connections" to be explained. Requirement also needs consideration for legacy devices v. the innovation greenfield.

Item #8 –

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

Edit text to: **"Default passwords must be prompted to be reset or changed on first use or uniquely generated, when sensitive data is collected.** Where possible, separate passwords should be required for administrative vs user access and not permit password reuse. Ideally passwords should be randomly generated."

Needs further development. See insertion on sensitive data.

Item #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.

At a minimum, edit text to: **"All user sites should 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."

Recommend combining #9 and #10 and remove reference to a specific protocol as they do age (concur with "age like fish" analogy [given]). Policy statements should outlive a particular technology. Suggest something like "…should use a secure protocol by default"

Item #10 –

> **All device sites and cloud services must utilize HTTPS encryption by default.** Also 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.

At a minimum, Edit text to: "**All device sites and cloud services should utilize HTTPS encryption by default, where sensitive data is collected."**

See comments in #9

Item #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.

Edit text to: "**Manufacturers should conduct reasonable penetration testing for devices, applications and services."**

Item #12 –

> **Manufacturers must have capabilities to remediate vulnerabilities in a prompt and reliable manner either through remote updates and / or through consumer notifications and 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.*

Appreciate the recognition of legacy devices. This appreciation should be more fully illuminated and applied more broadly to the entire list of recommendations wherever appropriate, perhaps in language preceding all recommendations.

Item #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 exercise

This is not an IoT issue and should be deleted. If a sufficient argument can be made to retain it guidelines should be consistent with PCI and SOX requirements – annual is sufficient. Comment about 3rd parties should not be

accepted. Of course as a practical matter organizations may choose to involve 3rd parties in their tabletop exercises if deemed appropriate.

Item #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.

Concur

Item #15 –

> **Device must provide a visible indicator or require user confirmation when pairing or connecting with other devices.**

Agree with comment that "human intervention should not be required" as there are designs specifically done to eliminate the need for a human interaction which in certain applications this enhances security. Additionally, visual indicators create a battery issue.

Recommend its deletion.

If retained, suggest limiting to Terms of Service statement that provides consumer transparency around pairing.

Item #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.

Concur with this as an aspirational design standard

Item #17 –

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

This should be deleted. It is not a priority. It may be useful at some point as a design feature for product differentiation (vs a security or privacy mandate). Application to enough home automation devices to warrant its inclusion, is debatable.

[One] contributor continues to raise credentialing issues across several of his comments. Perhaps the points he is making suggest further review to see if credentialing guideline might be expanded and allow combination/deletion of a few of these latter draft guidelines

Item #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**.

This is valuable, but it is best left to the market place for product and customer service differentiation. "Regarding company issues including but not limited to…" makes the point. We are working on privacy and security top priorities, not on customer service issues.

Item #19 –

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

Disagree with the inclusion of recommendation in this trust framework. This is a business decision not a privacy or security consideration. There are IoT devices where the design purposefully accomplishes the opposite, i.e. a purposeful effort was made to not allow for this transfer to happen.

Item #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.** Capabilities should include ability to reset to the "factory default."

Not acceptable if intent is to provide these "controls" at granular level. "Must have" controls should be limited to discontinuing the service or device function; in that light, and in the spirit of having a manageable framework to seek consent, recommend its deletion.

Item #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.

Is this a privacy and/or security issue? Delete

Item #22 –

> **Manufacturers must disclose what functions will 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).

This is unclear to us. Delete. The door and garage door examples cited operate via traditional mechanisms (i.e. the OEM keypad for garage doors) whether the smart function is operative or disabled…so what is the problem this is addressing? Also how is "key home automation products" defined?

Item #23 –

> **Configure all security and privacy related email communications to 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. Additionally organizations should consider STARTTLS and opportunistic Transport Layered Security (TLS) for email to aid in securing communications and enhancing the privacy and integrity of the message.

Looking for clarification here. Is the intent is to protect communications to the customer that are specific to updating or reconfiguring the security settings of devices? Concur with other submitted comments recommending deletion of this item.

Additional Recommendation Items #1-12

Recommend none of the proposed "additional recommendations" be added at this time.