Consumer Federation of America
1620 I Street, N.W., Suite 200 * Washington, DC 20006

Comments to the Online Trust Alliance on the
IoT Trust Framework – Discussion Draft
September 21, 2015

Security and privacy are major concerns for consumers as they consider whether to adopt new technologies. While Consumer Federation of America (CFA) believes that a comprehensive legal framework is needed to provide consumers with enforceable privacy and security rights and clear "rules of the road" for businesses, voluntary guidelines can help to promote consumer confidence and encourage good industry practices. The issue of sustainability is also important to address. Consumers invest considerable time and money in high-tech products and services and want to be ensured that they can be updated as needed and will continue to function for a reasonable period of time.

CFA welcomes the initiative of the Online Trust Alliance (OTA) to develop best practices for manufacturers, developers and retailers on designing, creating, adapting and marketing connected devices (referred to as the Internet of Things, or IoT). The focus of the IoT Trust Framework (the framework), home automation and connected home products and wearable technologies for health and fitness, is timely because use of these products and devices is increasing and the data derived from them can be highly sensitive. The two subject areas raise some different issues, however, and it might be better to start with one or the other rather than both.

Before commenting on the specific provisions of the draft framework, CFA would like to offer some general observations. First, while the framework is aimed at manufacturers, app developers and retailers, the IoT appears to be headed toward a future in which there will be platforms operated by companies such as Apple, Google and Microsoft that will enable products and devices to communicate with each other and create a seamless network. ISPs and wireless telecommunications providers will also play a major role in the ecosystem, since most home automation and connected home IoT products need to connect to Wi-Fi networks in order to function. The framework must address these entities.

CFA notes that in some cases the requirements in the framework specify the entities to which they are directed, but in other cases it is not clear to whom they would apply. Retailers, though mentioned in the introduction, are not mentioned at all in the requirements. It would be helpful to specify to whom the provisions apply throughout.

It might also be useful to provide definitions of phrases such as "personally identifiable data types and attributes," "personal data," "third parties" and "service providers."

CFA also notes that while the framework is based on the FIPPs, it doesn't fully incorporate them. For instance, it does not require that consumers have access to their data. A more comprehensive embrace of the FIPPS would make the framework stronger, better, and more adaptable globally.

Finally, CFA believes that this is an opportunity to implement strong privacy and security principles while the IoT is still developing. The OTA and its members should be bold in their ambitions. There is no point in merely codifying current business practices or in guidelines that are so vague that they provide no real parameters for future practices. This is a moment to show leadership.

CFA Comments on Proposed Minimum Requirements

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, include the impact to usage of key product features and functionality.**

CFA supports this requirement. It is especially important for consumers to have the information about how exercising the privacy-related choices they are given will impact the use or functionality of the product. It would be helpful here or elsewhere, if more appropriate, to specify that the privacy policy should be in plain language and available in languages other than English.

It is not clear whether the framework would apply when the product is offered for free; for instance, if a consumer's utility company or insurer offers a device at no charge. Perhaps this could be addressed in describing the scope of the framework.

2. **The privacy policy display must be optimized for the user interface to maximize readability.**

CFA supports this provision. In some instances, however, there will not be a user interface. This should be addressed.

3. **Manufacturers must conspicuously disclose all personally identifiable data types and attributes collected.**

It might be useful to say "clearly and conspicuously disclose…" here. This provision should apply to any entity that will collect data directly from the device. It should be required to disclose that and describe the types of data or attributes involved and how it will be used.

4. **Any default personal data sharing must be limited to third parties /service providers who agree to limit usage for specified purposes.**

CFA finds this provision rather confusing and convoluted. It conflates third parties and service providers, which are not always the same. There should be a core principle that personal data should not be shared with any third parties without the consumers' affirmative consent, with an exception for service providers that need certain data in order to perform functions that are directly related to the products or services that the consumers have requested. Thus, this provision could say:

"Application developers or manufacturers should only share consumers' personal data with third parties with their affirmative consent, except that such data may be shared by default with service providers as needed for the purposes of supporting the product features and functionality, improving the product, or delivering the services that the consumers requested.

Service providers' use of consumers' personal data must be limited to those purposes, unless the consumers have affirmatively consented to other uses. In order for any third party to receive and use consumers' data for other purposes, the application developer or manufacturer must provide a clear explanation of what data will be shared, with what type of entity it will be shared, and how it will be used, and obtain consumers' opt-in."

CFA also recommends that this provision should state that consumers should not be required to agree to third party sharing where it is not necessary in order to provide the services that they have requested.

In addition, CFA notes that there is currently no provision in the framework for seeking consumer consent for uses of the data by the application developers or manufacturers themselves for purposes that are not necessary to provide the services that the consumer has requested. CFA believes that such unexpected uses should not merely be disclosed in privacy policies; consumers' affirmative consent should be required.

Again, perhaps this section should be directed at other entities as well.

5. **The term and duration of the data retention policy must be disclosed.**

CFA supports the requirement to disclose the data retention policy. It is not clear, however, whether it *requires* deleting the data upon expiration or account termination, except as retention may be needed to meet legal requirements. CFA believes that it should.

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.**

CFA finds that this provision falls short in a number of respects. It should apply to any entity that collects data directly from the device. It is unclear what is meant by sensitive data. CFA believes that consumers should be given the ability to ask for data to be

deleted at any time, not just when they are no longer using the device, if that data is not necessary for its functioning. Furthermore, consumers should have access to their data.

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.**

CFA supports these security requirements. It might be useful to note that as security technology changes over time, there may be improved security measures that should be adopted. It is not clear if third parties are covered by this provision.

8. **Default passwords must be promoted to be reset or changed on first use or uniquely generated.**

CFA supports this provision.

9. **All user sites must adhere to SSL best practices using industry standard testing.**

CFA supports this provision.

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

CFA supports this provision. It might be better to say "wherever possible," however, since this may not always be possible globally.

11. **Manufacturers must conduct penetration testing for devices, applications and services.**

CFA supports this provision.

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.**

CFA supports this provision. It might be useful to specify that instructions should be designed to be easy to follow, available in multiple languages, and that support should be available, if needed. It seems as though this should apply to application developers and platform operators as well.

13. **Manufacturers must have a breach response and consumer safety notification plan, at a minimum reviewed semi-annually.**

CFA believes that this should apply to all entities that hold the consumers' personal data.

14. **Manufacturers must provide secure recovery mechanisms for passwords.**

It seems as though this should apply to application developers as well.

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

This is an important provision. CFA wonders if both a visible indicator and user confirmation should be required.

16. **All updates, patches, revisions, etc. must be signed/verified.**

CFA supports this provision.

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.**

CFA supports this provision. There must be the means for parental/administrative control, especially to protect the personal data of children.

18. **Manufacturers must public 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.**

CFA wonders if it would also be useful to require application providers and platform operators to provide mechanisms for contact.

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

CFA agrees that this is especially important for connected home devices and wonders if application providers and platform operators should have similar obligations.

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.**

CFA again supports this provision and wonders if application providers, platform operators and ISPs should have similar obligations. The controls and documentation should be prominent, not buried or hard to find. The documentation should be available on the website as well as at the point of contact with the device.

21. **Manufacturers must publish to consumers a time-frame for support after device/app is discontinued or replaced by newer version.**

CFA agrees that it is very important for consumers to have this information but the reference to "This…should be for the life of the device" is confusing. It seems that this information should be available for a reasonable time after the device has been discontinued or replaced by a new version.

22. **Manufacturers must disclose what functions will work if "smart" functions are disabled or stopped.**

CFA believes that this information is absolutely critical and agrees that core functions must remain operative and that for key home automation products, there must be a back-up mechanism for access and use in the event that connectivity is lost.

23. **Configure all security and privacy related email communications to adopt email authentication protocols.**

CFA supports this provision. The framework does not mention other means of communication such as robocalls and texts; it might be useful to have an additional provision that promotes compliance with the applicable privacy limitations and requirements.

<u>CFA Comments on Additional Recommendations</u>

CFA strongly urges the OTA to move the following "additional recommendations" to the "requirements" section because they are sufficiently important to be mandatory rather than mere suggestions:

- The transfer of consumer data in the sale, merger or liquidation of a business. This should follow the guidance that the Federal Trade Commission has established through its legal actions and interventions in this regard.

- Preventing personal data that has been de-identified (this is more accurate than saying "anonymized") from being re-identified, and data minimization. These are well-established principles.

- Making material changes to privacy policies. This should follow the guidance from the FTC that material changes affecting data which was previously collected requires consumers' affirmative consent and that material changes concerning personal data collected going forward requires clear notice.

- The ability for a consumer to return a product without charge after reviewing the privacy practices that are presented during initial set up. This is an excellent best practice and would ensure that consumers can truly exercise privacy choices.

- The provision that manufacturers optimize device interface and usability for users with various physical impairments. This should probably apply to apps as well.

For questions concerning CFA's comments on the OTA draft framework, please contact Susan Grant, CFA Director of Consumer Protection and Privacy, sgrant@consumerfed.org.