May 2013

# Input on the privacy and security implications of the Internet of Things

## Executive Summary:

Dear Reader - The comments below have been crafted by a set of Kantara Initiative Trustees, Members and Participants that represent a reasonable cross-section of jurisdictional and industry expertise. The comments included were collected and edited transparently and on a volunteer basis where all Trustees, Members and Participants had reasonable opportunity to provide input. However, the statements below do not reflect the opinions of Kantara Initiative as a whole. We thank the Federal Trade Commission for the opportunity to participate in a broader discussion of security and privacy implications of the Internet of Things. Responses to this submission may be addressed to staff@kantarainitiative.org.

Best Regards,

Joni Brennan
Executive Director
Kantara Initiative

## Detailed Responses:

**What are the significant developments in services and products that make use of this connectivity (including prevalence and predictions)?**

The next important developments in the Internet of Things (IoT), rather than specific products or services, should be overarching standards, policies, frameworks and infrastructures (apart from the internet layer). Each component would benefit from representation in an overall architectural model that would enable visualization of how IoT works as a part of and within systems. Such an architectural model would include a model that describes the components or elements of the "things" that are part of the IoT. Standardized interfaces and protocols enable the connection of solutions that are to date still rather isolated in nature. Through the development of open, industry, and market driven technical standards and binding policies, various services can be combined to create new ecosystems.

New eco-systems considerations include:

- The identity of the device
- Other data contained in the device
- Any binding of human identity to the device
- Access control information identifying what another entity is permitted to do (e.g., a device manufacturer is allowed to see operational/maintenance data, the owner is permitted to see all data, etc.)

Privacy and security risks will increase because information about things, or even knowledge about the existence of things and their identity, will be exchanged much more extensively. It is suggested that the development of a of a panoramic view in this space with regard to standards, policies and frameworks would help to optimize approaches to the implementation of the Identity

445 HOES LANE, PISCATAWAY, NJ 08854 USA
Phone: +1 (732) 465 5817 Email: staff@kantarainitiative.org

WWW.KANTARAINITIATIVE.ORG

of Things (IDoT) as a component of the IoT. IDoT is not only concerned with the identity of a thing (object) but also the binding of a person (i.e., an owner) or an organization (i.e., the manufacturer, the maintenance company) to an object.

The IoT and IDoT can bring many opportunities. If privacy and security is ensured, objects can communicate with each other or with human identities. This type of development would enable myriads of new apps, services, and business opportunities. In essence an IoT economy may be a new ecosystem that is spawned from IoT technical and policy standardization.

Finally, issues touching privacy and security will also have a strong intersection to Access Control practices and policies. Not only must data be protected by appropriate information systems technology and practices; detailed review and approaches should be defined with regard to considerations and application of Access Control to data associated with and/or gathered through IoT and IDoT means.

**What are the various technologies that enable this connectivity (e.g., RFID, barcodes, wired and wireless connections)?**

While RFID, barcodes, wired and wireless connections seem apparent in terms of connectivity, there may also be the addition of SIM cards and, in more general terms, Secure Element via mobile devices. Secure Element and Trusted Zones could prove, as another form of technology that is already widely deployed, to be supportive to IoT secure connectivity. Regardless of the current, or currently envisioned, technologies, all standards, frameworks and infrastructures need to be flexible enough to allow new technologies to be incorporated. The architectural model and the open standards, policies and frameworks suggested previously would ensure that the IoT is open to technologies and services that have yet to even be thought about.

**What types of companies make up the smart ecosystem?**

The types of companies that could make up the Smart Ecosystem include, but are not limited to, companies that produce products that would be part of the IoT, companies that operate services that would connect products and humans in the IoT, and companies that create measurement tools (like meters and testers). Any company where such tools could provide valuable operational data back to IoT networks and also help to make sure they are configured in a way to meet operational, privacy and security considerations are viable candidates. However, all data collected must be and protected for privacy and security considerations including, where appropriate, anonymization.

Note that companies are not the only possible source of data in the ecosystem. Another model that may be applied has the individual serving as the primary data generator feeding information into the IoT, with companies being the consumer of information rather than the aggregator and disseminator.

**What are the current and future uses of Smart Technology?**

Future uses for Smart Technology are bounded only by the imagination of innovators as well as the tools available and the best practices and legislation which govern those tools and their use. Areas where industry and end-users stand to gain huge benefit from Smart Technology include, but are not limited to: healthcare, utility metering, logistics, manufacturing, security products and services, and retail.

In addition to these possible future uses, it should be clear that variants of IoT, with some approach to Identity Management practices, are already operating today. One clear example of an existing use case is that of Electronic Toll Collection (ETC). This technology is already pervasive on many highways around the world and is continuing to advance with many of the smart vehicle initiatives underway. This is an example of previous military "friend or foe" technology being put to reuse for public sector implementation. The digital "pass" links to an associated account to draw payments. Note that there is no binding of who was actually driving. The Authentication and Authorization occurs at the device level. This system is participatory by choice as there are still cash lanes at each exit. This use case illustrates that IoT (i.e., security, privacy and access control) are not completely new applications of technology. However, it is the pervasiveness of technology application that will change moving forward.

Thought and consideration should also be given to the applicability of current, or emerging, Access Control best practices, approaches and technologies (e.g., attribute based access control). Thought should also be given to how authentication and identity management practices that are currently being applied to individuals might be evolved to apply to devices – the things of the IoT.

**How can consumers benefit from the technology?**

Individuals may benefit in many ways from the implementation of the IoT. They may save time and money. They may gain more convenience with regard to operations and transactions.

Examples:

- Medical patients may benefit from not having to spend the night in a hospital while their smart phone is performing tests and monitoring remotely. These technologies are in limited use today.
- Homeowners may no longer need to create grocery lists as their favorite groceries will be inventoried and owners will know exactly what goods are needed to stock the refrigerator.
- Grocery stores may have trusted relationships with homeowners such that needed goods are delivered automatically to the home once per week or as necessary.

**What are the unique privacy and security concerns associated with Smart Technology and its data? For example, how can companies implement security patching for smart devices? What steps can be taken to prevent smart devices from becoming targets of or vectors for malware or adware?**

There should also be assessments, as part of the development of the architecture of the IoT, to identify the types of information that may be associated with a thing including any security and privacy risks arising from the thing being part of the IoT. In addition to technical security mechanisms we see object identity specific privacy risks such as:

- An object is associated with the wrong identity information. This could lead to consequences ranging from confusion of services up to severe errors. (e.g. decisions are made upon results that are taken from a wrong sensor)
- Identity information about an object is inaccurate or out of date. (e.g. device cannot communicate anymore)
- Identity information of an object is asserted by parties that are not considered as authoritative.(e.g. someone proofs that a certain device fulfills the requirements that is not entitled to)

- Object Identity information may be used by someone other than its rightful or authorized owner (e.g. a burglar could request status information of a home-automation system in order to see if someone is at home)

**How should privacy risks be weighed against potential societal benefits, such as the ability to generate better data to improve healthcare decision-making or to promote energy efficiency? Can and should de-identified data from smart devices be used for these purposes, and if so, under what circumstances?**

While pervasive deployment of the IoT may be a relatively new concept, it may be beneficial to draw upon the methods and practices of established infrastructures including Public Health Agencies that draw data (anonymized) from hospitals and doctors to address public health concerns. Precedence may have already been set in the medical field that it could be extended, with proper legislative oversight, to other fields.

User consent is paramount in the case where persons and objects will be linked to each other. Scenarios quickly become Identity focused and therefore securing user consent will make implementation of smart technologies easier. Current paradigms for user consent suffer from poor implementations and a lack of real consent, leaving this area ripe for different models. While IoT and IDoT are ready for implementation today, we continue to express the need for a panoramic view of open industry standardization. Implications of IoT are not fully understood and should be explored by Standards Organizations and Industry Consortia so that truly strategic roadmaps can be developed.

A reasonable gap between legislative mechanisms concerning Privacy already exists between many countries (i.e., the EU, Canada) and the US. Implementation of IoT in isolated approaches serves to exacerbate this issue and could potentially drive the user away from using products and services that implement the IoT. IoT must be deployed as a beneficial service to individuals and citizens and not be imposed upon them. In order to address these risks it is envisioned that there would be series of pilot projects that could be used to research, use case prove, and optimize conceptualizations regarding IoT standardization. With a combination of “speed-to-market” pilots and deliberately pragmatic studies done by Standards and Industry consortia, IoT would have most optimal opportunity to be deployed for the benefit of the broadest set of users.