This email is written in response to your request for comment (RFC) regarding "the benefits, challenges, and potential roles for the government in fostering the advancement of the Internet of Things (IoT)." This response represents the opinions of the undersigned only.

Overview

The concerns regarding IoT technology are well stated in the RFC. It is clear that the NTIA is attempting to seek how to continue to foster and support growth in IoT devices/technologies without (a) being overly burdensome, (b) shirking governmental responsibilities re: proactive prevention of malfeasance or harm, or (c) stifling innovation. In this endeavor, I suggest that the government's principle roles should be to:

- Appropriately define data, information, and intelligence (derived information) within the ecosphere
- Provide clear use cases where data and/or information migrates into prohibited/protected space (and requirements for same)
- Set higher, clearer standards for obtaining consent from users regarding the use of IoT data, and
- Ensure that IoT devices which have the potential for collecting data that may be used in a prohibited/protected manner have the ability to be easily integrated into existing security frameworks.

Definitions

Before continuing with this discussion, it is important for us to draw some distinction between data, information, and derived information (or intelligence). Data are facts and statistics. Information is data in context. One example of this would be to look a 10-digit number (3015553079). This is a piece of data that currently has no context. We can attempt context to this data in a multitude of ways, each of which produces different information for the observer:

- 3,015,553,079 A number in excess of 3 billion
- 30 15 55 30 79 A set of 2-digit numbers
- +(30) 1555 3079 Part of an overseas phone number, possibly for Greece
- (301) 555-3079 A US telephone number

Let's assume that the last context is, indeed, the correct one. We now have information that we did not have before. Now let's add some additional pieces of information to the mix:

- (301) 555-3079 A US telephone number
- (301) An area code for Maryland
- Me I lived in Maryland in the late 90s

By combining these pieces of information we can derive the additional information that this might be an old phone number of mine.

Issues and Concerns

Data

As with most technologies in this data-driven era, the major concerns regarding IoT technologies should center around:

- The use of the data/information collected by those technologies
- When that data/information transitions into a protected/prohibitive use-case, and
- Potentially prohibitive use cases where derived information is created from data/information collected via IoT devices.

Some relevant (and not too farfetched) examples are as follows:

1. The simplest example centers around biometric/activity data collected in personal fitness tracking devices worn by millions today. While the activity tracker tracks my heart rate for my own personal fitness needs, what happens when a paramedic uses that heartrate tracker in an emergency situation to monitor a patient's vital signs as a caregiver administers treatment? The activity tracker itself is not considered a medical device (nor should it be, in my opinion); however the data obtained from that medical device may transition into use for medical purposes in real time. Does this impose a need for additional protections/control over that data?

2. A use case flowing from the aforementioned example would be whether or not a medical company might request the cloud-stored biometric data initially collected from this same activity tracker to help diagnose a patient that is no longer able to communicate on his/her own. Is this allowable? If so, does this potentially place the biometric data into the realm of Protected Health Information and force the device developer into complying with the related regulations (such as HIPAA, HITECH)? Do the devices themselves need to be certified by an independent or governmental body to ensure the collected data is accurate — especially as life and death decisions are made based on the collected data?

3. Can data from my activity tracker be sold to an insurance company and used to make coverage decisions?

4. My favorite example is the one I refer to as the "Joker Toxin" example (see https://www.youtube.com/watch?v=mXV9I9okrNs for an explanation as to why I use this title). Is there a use case where combining the freely given data from a multitude of IoT devices creates relatively "toxic" derivative information on a subject which must meet higher standards of protection?

5. The amount of data generated via a plethora of IoT devices can create a holistic surveillance picture on an individual. Are we, for example, comfortable with the idea that a surveillance effort that compromises the wireless network of a suspect now potentially provides access to more and more information from the suspect and his/her activities? While clearly a surveillance operation of this sort would be minimally invasive, is the amount (and type) of data so excessive that it merits additional considerations before authorizing the operation?

Identifying potentially toxic use cases, determining which such use cases transition data into a protected space, and placing appropriate (yet minimally restrictive) controls around IoT-collected data is an effective and appropriate role for a government entity — and solves a problem that reaches well beyond IoT devices.

Consent

We have entered an age where both consumers and retailers are striving for personalization. In order to meet this demand, consumers are increasingly willing to part with their data… which retailers/businesses are increasingly eager to consume/analyze. The argument most often made when questions are raised around use of data is that the consumer has consented to the use via the end user license agreement (EULA). While this provides a level of legal protection on the part of the corporation, is has been widely shown that most users do not read the EULAs presented to them. With the continual disclosure of data that is occurring, there is a risk of consumer backlash if "toxic" derivative information is released/disclosed from otherwise mundane IoT-collected data. The industry should be pushed to clearly disclose — in simple terms that are easy to digest — exactly what data is collected, how the data collected will and will not be used, and with whom the collected data will be shared.

Security

Your RFC appropriately pointed out the challenges regarding security that exist within small, innovative companies. Placing a plethora of security controls on IoT manufacturers is not realistic, nor will it foster the innovation that

you are seeking around IoT. That said, ensuring that IoT devices have the capability to be secured (e.g., using standard data transmission formats and secure ports/protocols, as well as the company having a program and infrastructure to track vulnerabilities, remediate them, and deploy patches) will ease the burden of integrating IoT devices into secure environments.

Point of Contact

Point of contact for this submission is the undersigned.

Kim L. Jones CISM, CISSP, M.Sc.
Director, Cybersecurity Education Consortium
Arizona State University
(602) 543-6038 (o)
KimJones.CISM@asu.edu