**NTIA Consultation on Big Data:**

**Submission from ARM Holdings**

## Introduction

ARM designs microprocessors, used in 95% of mobile phones and many other products, including servers. We are a global company with operations in the US, East Asia and other parts of the world. Our Headquarters is in the UK.

We have a strong interest in the Internet of Things (sometimes known as Cyber Physical Systems) and therefore in how data can be used to help drive IoT.

Some argue that the business models for IoT will rely heavily on being able to monetize data, and/or use it for public policy benefit. It is important to us therefore that any approach to data reconciles the two imperatives of sustaining public confidence in how data is handled and used, and at the same time, stimulating innovation in data usage. We believe that, properly managed, data can drive economic growth.

## Big Data starts with Little Data

Big Data is the agglomeration of many little pieces of data. This is already happening: data about what online sites consumers visit, what purchases they make, what their health apps record, is capable of being aggregated.

This will increase as the Internet of Things (IoT) revolution gathers pace and many objects have embedded sensors sending information about their environment or themselves to another object ( eg mobile phone) for analysis and action. In many cases it is expected that the data will end up in a Big Data storage center in the Cloud.

Influential estimates predict that billions of devices will be connected in this way.

## Our Approach

ARM has worked with AMD to draw up some principles to guide the data debate. We believe that these principles can underpin a responsible use framework. We have not been able to address all the specific questions in your call for responses in the time available to us, but would be happy to provide more detail later.

Our hope is that the principles we have outlined will form the starting point for an industry led conversation about a framework designed to give consumers confidence in how their data is handled.

## Six Principles for the IoT Data Discussion

We propose the following policy principles as a starting point to guide policy discussions for securing and maintaining privacy for IoT data.

- **Technology Can Help**

It is useful to distinguish data security from data protection. The former aims at ensuring data cannot be intercepted en route to its authorized destination; the latter refers to how an authorized recipient might use data.

Effective IT security features and technology solutions are the first and final defense against malicious intrusions and cyber-attacks. Robust, open standards-based approaches to IT security that promote interoperability are the most efficient means to ensure broad coverage and widespread adoption.

We are working together with other partners to advance the ARM® TrustZone® technology. TrustZone® allows consumers and businesses to secure their data and perform secure transactions, such as banking transactions, with a much greater level of trust and protection than current technologies.

- **Not all data is equally sensitive**

Data sensitivity varies according to type of data, context etc. For example, consumers may be content for their data to go to certain recipients but not others: you might be happy for your health data to go to your doctor but not to your insurance company.

Second, provided the chain of custody is secure, consumers may be happy to share their data with a number of recipients who could use it to offer new services, provided it does not fall into the hands of people who might misuse it (for identity theft, or to track movements etc.) or use it in ways consumers are uncomfortable with.

Finally, anonymized data is likely to be less sensitive than identifiable data.

It follows that one approach to a responsible use framework might start from the notion that different types of data should be managed differently. By establishing specific categories of data and associated responsibilities and mechanisms to manage each category of data, a framework can be established that provides an efficient means of addressing data security and protection.

For example, the following types of data could be managed differently:

(i) Highly sensitive data – health, financial, individual communications, trade secrets, etc;
(ii) Volunteered data in context of a transaction or enabled via consent (i.e. Opt-In);
(iii) Observed data about one's interests, activities, movements, etc. that is collected with one's consent (i.e. Cookies);
(iv) Observed data about one's interests, activities, movements, etc. that is collected without one's consent (i.e. web trackers); and
(v) Anonymized or de-identified data (i.e. anonymous surveys).

Highly sensitive data must be fully protected with very high assurance. Data that is volunteered, depending on the instrument and context, may be less sensitive and require a lesser degree of protection and assurance. Similarly, data that is anonymized or de-identified, assuming assurance that it has been sufficiently anonymized or de-identified, is much less sensitive than data associated with a specific individual. In short, establishing such a framework can help target the specific level of security and privacy protection that is appropriate for different types of data.

- **Consumers should own their own data**

Work on data by the World Economic Forum (WEF) suggests another approach to considering the sensitivity of data:

(i) data volunteered in the context of a contact or contract;
(ii) anonymized data (e.g. “How many cars are in a traffic queue based on mobile phone signals?”); and
(iii) between these two, data which is observed about someone without their knowledge, whether directly or through the transfer of their data to a third party.

Over time, we could aim for categories (i) and (ii) to expand, thus reducing category (iii) about which there is most concern.

This will require consumers to be more aware of the fact that they should be able to determine what is done with their data: in short that they own it. We believe that consumers may be willing to share more if they are better informed about how their data is being used and what the benefits are (individually or more widely).

No one yet has the right answer to this. Below, we offer some thoughts on some of the issues involved. These,too, may contribute to the design of a responsible use framework.

The key to giving consumers more control over their data usage may be to simplify Terms and Conditions, ideally into a series of simple descriptions which cover key types of data usage. These could possibly appear as a ‘traffic light’ series of explanations (and options) when consumers sign up to a new service or, eventually, maybe as a default setting on their device.

(This would presuppose a shift in the focus of the debate from data collection to data usage.)

In drawing these up it may helpful to distinguish between certain key uses of data. There may be two broad use scenarios:

(i) **consumer as target**: this is where the aim of assembling and analysing data about a consumer is to offer them additional products or services.

In some cases these offers will be directly linked to an action a consumer has taken on line (researching specific products or entering into a specific contract). In some cases it may be the result of drawing inferences ( eg about a consumer's life style based on various sources of information).

(ii) **consumer as topic**: this is where the primary aim of analysing data is to generate a 'conversation' about the consumer.

The sorts of situations this includes are where, without your permission, your health data is sent to your insurer, or your employer, or your financial data goes to your mortgage company or employer etc. It also includes particularly sensitive situations where data is used to make sensitive 'predictions' about a consumer's health etc, or to categorise consumers in ways consumers may not approve.

Consumers are likely to be much more sensitive in general about (ii).

Taking these two scenarios together it is possible to envisage a scale of explanations/options for data usage as follows:

(i) Your contracting party or a third party use your data related to this contract/contact to help maintain your product/ service
(ii) Your contracting party or a third party use your data to inform you of other similar products/services, and a variety of different products/services based on an inference about your life style.
(iii) Your contracting party or a third party use your data to generate a profile about you, including predictions of situations in which you might want to know about a variety of different services.
(iv) Your contracting party or a third party make best efforts to keep your data anonymised so that it can be used for a variety of marketing or social policy analysis.
(v) Your contracting party or a third party use your data for any other reason.

**• Consumers must have confidence in how their data is used, stored, and transported**

More needs to be done to reassure consumers about the security arrangements for (i) protecting their data against hacking and

(ii) ensuring their data is not wrongfully transferred to an unauthorized recipient. An important aspect of this is informing consumers of the benefit they gain from agreeing to their data being used in various ways.

- **Data can drive economic growth, and provide a multitude of societal and individual benefits**

Data can have significant economic benefits and help to drive wide economic growth. It can also help improve delivery of services in health, environmental management, smart cities etc.

- **A data-handling framework that categorizes different types of data and associated management strategies is required to unlock the potential of IoT**

This needs to bring together specific proposals on how to put these principles into practice. Its aim should be to reassure consumers while at the same liberating data to drive innovation.

Conclusion

Clearly, there is a great deal of work that needs to be done to address the security and privacy issues raised by the Internet of Things era. But just as clearly, the IoT era is already providing tremendous benefits, with the promise of truly transformational change and benefits going forward for individuals and society as a whole.

August 2014

ARM Holdings

Stephen Pattison, VP Public Affairs