Data Management in the Internet of Things (IOT) Era

Common Policy Principles and Data-Handling Framework for Data Security and Privacy

ARM and AMD

There has been much talk about "The Internet of Things (IoT)," but still no widely accepted clarity about what it means. In our view, IoT is simply the ability for common devices and sensors to collect information about what is happening to them or around them, and to communicate it elsewhere, often to people, who can then act upon it. We see it as a game-changing development in the ongoing evolution of information technology and the global economy.

Computing and networking technologies are evolving at a rapid pace, driven by increasing demand for "anytime, anywhere" access to data and services, as well as technology innovation that is enabling a wide array of new electronic products. Examples include electronic medical devices that are able to remotely connect doctors and patients to treat life-threatening or chronic conditions; "smart grids" for utilities that help consumers manage their energy use; networks of sensors that can provide real-time information on traffic conditions on highways, or help protect the safety of schools and neighborhoods; and personal "smart devices" that people can carry or wear so they can easily access the data and services they use at home, at work and at play.

A key point about IoT is that it will enable us to use our resources more effectively. It will help us waste less water and less energy. It will help us calibrate more carefully how we manage our streetlights, our buildings, our traffic flows. It will enable us to improve health services and derive more and better health related data. In essence, IoT will help us communicate more effectively.

People around the world, from all walks of life, are already benefitting from the improvements delivered by networked technologies. So too are businesses, governments, educational institutions, and other organizations that are able to use, combine and package data in ways that create new products and services, generate operational efficiencies, enhance service delivery and drive economic growth. As technology innovation continues to improve and evolve for "The Internet of Things" and "Big Data" related technologies, so will the benefits they are able to deliver, as well as the possibilities that they promise for the future.

Of course, any new technology poses challenges. Think of the introduction of the motor car and the debates that must have prompted about safety, cost, etc. In the end, 'rules of the road' resolved anxieties and liberated the car to transform our lives. We may be at a similar point with IOT.

The sheer scale and pervasiveness of IOT networks, devices and applications presents considerable challenges for ensuring consumer confidence in how their data is handled. Complex, interconnected information technology ecosystems, involving legacy systems connected to new networks and security applications loaded on top, sometimes as an afterthought, do not make the challenge any easier.

While the challenges are considerable, the good news is that the security technology and solutions market is rapidly growing to meet the security issues presented by IOT and other related IT trends in mobile and cloud computing, as well as Big Data applications. As a result, there is a major security focus and an increasing number of standards and requirements that have been developed and are being implemented in the IT ecosystem.

From the perspective of ARM and AMD, as well as many of our customers and partners, hardware-based security features that compliment applications and network level security capabilities are a fundamental component for creating a truly secure information technology ecosystem.

AMD, a global leader in CPU and GPU design, and ARM, the largest processing technology company for the mobile device markets, 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. This industry collaboration will help accelerate broader ecosystem support by aligning x86 hardware – the current computing industry standards – with the world's most broadly-adopted mobile security ecosystem – ARM-based technologies.

We're making good progress in providing secure technologies, but we also realize that rapidly evolving security threats online cannot be addressed by any one company, standards body or government. The job is too big for anyone to do alone and protecting data and privacy is a shared responsibility. As cybersecurity challenges continue to evolve, we can't point to others to solve the problem. We need collaborative industry development and public-private partnerships to more fully secure cyberspace.

ARM and AMD commend the FTC for their foresight in considering potential security and privacy issues related to IOT technologies. While we would caution against imposing new regulations or restrictions that may be premature or have unintended consequences at this early stage of the IOT era, we do believe that a robust and thoughtful discussion of policy issues is important to ensure that data security and privacy issues are thoroughly explored and addressed.

Specifically, we believe that the correct approach to the discussion should consider the following **key points**:

1. ***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.

2. ***No single technology, industry standards body, public policy, or government agency can fully address the rapidly evolving security threats in cyberspace.*** The entire IT ecosystem, industry standards bodies, government regulators and enforcement agencies, and individual consumers and businesses must all assume responsibility for securing cyberspace and protecting data and privacy.

3. ***A common set of policy principles and a framework for data-handling is needed for policy discussions.*** Industry bodies, government agencies, technology consumers, and other stakeholders need a shared understanding of key policy issues and approaches to data security and privacy so that policy discussions can be effectively and productively pursued.

Six Principles for the IOT Data Discussion: ARM and AMD propose the following policy principles as a starting point to guide policy discussions for securing and maintaining privacy for IOT data.

- **Consumers should own their own data**

Work by the World Economic Forum (WEF) suggests online data falls into three categories: (i) data volunteered in the context of a contract; (ii) anonymised 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 should 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.

- **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.

- **Not all data is equally sensitive**

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 you 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.). Anonymised data is likely to be less sensitive than identifiable data, particularly where it is clear that anonymised data is used for public benefits.

- **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 unauthorised recipient. An important aspect of this is informing consumers of the benefit they gain from agreeing to their data being used in various ways.

- **Technology is a significant part of the solution**

ARM is working on several areas to improve the security of data, and to enhance consumer confidence in having control over their data.

- **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.

An Initial Idea for a Data-Handling Framework: 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 should 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.

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.

We greatly appreciate the opportunity to share our ideas, and we look forward to continuing to work with our industry and government peers to usher in the IOT era in a manner that fully respects individual rights to privacy and provides strong security and protection for sensitive data and IT assets.