Privacy Implications of the Internet of Things

Ken Figueredo @ www.*more-with-mobile.com*
30 May 2013

Historically, the term 'Internet of Things' (IoT) has been linked with the application of RFID[1] technologies. RFID tags have long been used to track manufactured goods in supply chains and to manage stock inventories, for example.

Nowadays, the IoT term is used more broadly and belongs to a family of terms that include M2M, connected devices, Internet of People and Internet of Everything. Collectively, these terms encompass a wide variety of connected industrial and consumer devices that employ different forms of wired- and wireless technologies to transmit electronic data.

Affordable connectivity has significant improved prospects for the IoT

Connectivity has increased the range of sources and also the amount of data available for new service concepts. Now, data can be used to monitor and model the behaviors of machines and individuals. Such models act as a stepping stone to the implementation of predictive analytics. In the case of connected machines, for example, it is possible to forecast when a machine might be on the verge failing so that timely maintenance can be scheduled. Similarly, inventory data from vending machines can be used to organize replenishment schedules and even to fine-tune each vending machine's product mix based on local patterns of consumption. A third example is where consumers are targeted with promotional sales offers based on demographic, behavioral and location data derived from mobile phones and other connected devices.

The increased availability of data, collected at frequent and regular intervals, also lends itself to time series analysis as well as closed-loop business strategies. While closed-loop control is a well-established discipline for industrial control systems its application in the consumer arena is gradually starting to take hold. This has been made possible by the advent of remotely connected devices, new functionality due to higher performing microprocessors in connected devices, and ease of control through Smartphone and Tablet interfaces.

The mobile industry has had a significant influence in the resurgence of IoT. The following three characteristics stand out:

- consumer ease-of-use which has led to a wider acceptance of connectivity technologies across virtually all demographic groups,

- economies of scale which have fostered affordable products and services across the income spectrum,

[1] RFID (radio-frequency identification) involves the use of tags that contain electronically stored information. These tags are used to transfer data using a non-contact, wireless approach for the purposes of automatically identifying and tracking tags attached to objects.

- and, ubiquity of coverage which has increased the degree of reliance businesses and consumers place on communications and information services.

These trends have helped to propel the IoT market by building on the momentum around M2M (machine to machine, primarily for industrial applications) and Connected Devices (primarily involving consumer electronics types of device for entertainment, personal wellness monitoring, home automation etc.).

The IoT market has also gained impetus from advances in the capabilities and increasingly affordable price-points of short-range wireless technologies such as Bluetooth, Wi-Fi and ZigBee.

New business roles will emerge in the IoT eco-system and value-chain

Several entities are involved in delivering a connected device service to end-users through the following type of value chain.

Figure 1 Simplified representation of an M2M value chain

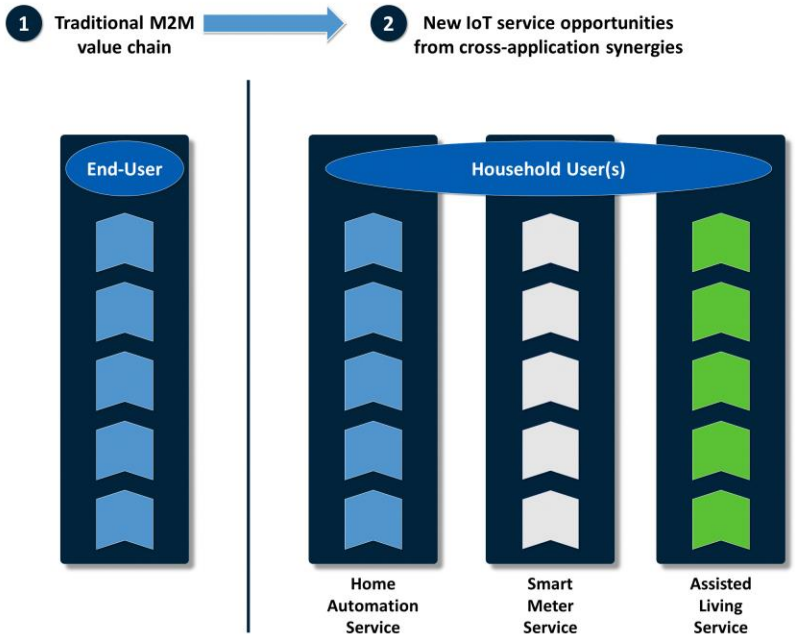
The organizations involved in this value chain are wireless module technology and wide-area connectivity providers. These two entities allow a device provider, such as a vehicle, vending machine or health-sensor manufacturer, to create a connected device. The connected device provider, or some other entity, then creates and supports an application based on the connected device to deliver a service to an end-user.

In practice, the illustrative value chain above varies from one application to another for a variety of reasons related to application specific requirements, distribution channel models and the size of the total addressable market. As a result, M2M and Connected Devices markets tend to exist as silo or single-application markets. For example, a fleet telematics application could be provided by an applications developer on behalf a road haulage operator seeking to track its vehicles and to optimize its route network. This solution and value chain would not necessarily be the same in another enterprise sector or a consumer applications example.

In the case of IoT applications the service permutations are considerably greater and the value-chain correspondingly more complex. This is because IoT service applications make use of data from multiple sensors and connected devices that may initially have been deployed for separate and unrelated purposes.

To illustrate this point, the following illustration shows the case of a set of services delivered in a home. These services – home automation, smart metering and assisted living – would each be deployed for a specific application purpose by businesses in three separate value chains. The ability to combine data across the three vertical services in this example could result in a higher quality of services (through improved information integrity) as well as new service opportunities (e.g. home security, wellness monitoring).

Figure 2 IoT Value Chains Will Create Opportunities for New Services and Data Providers



SOURCE: more-with-mobile.com (2013)

In contrast to the M2M value chain, the emerging IoT service delivery model will create new entry points in between component value chains. Typically, there will be new roles for organizations that aggregate end-user and sensor data from connected devices that belong to or are associated with individuals.

Such organizations will operate across horizontal layers along different application specific value chains. This will be simplified if data gathering and reporting capabilities are designed into modules, connectivity management platforms, and devices by default. Two examples illustrate how this might occur at different points in the value chain.

1. **In-the-Middle (ITM) IoT data brokerage** – at the network connectivity layer, tracking of a driver's mobile phone and other in-vehicle connected devices (navigation device, vehicle telematics device etc.) can be used to measure traffic patterns and route congestion. This data can be monetized in traffic alert and route optimization services.

2. **Over-the-top (OTT) IoT data brokerage** – this example applies at the end-user layer in the service value chain. Here, data from credit cards, smart payment cards and mobile wallets can be analyzed for purchase information and used to inform consumers about location specific prices for fuel and other consumables.

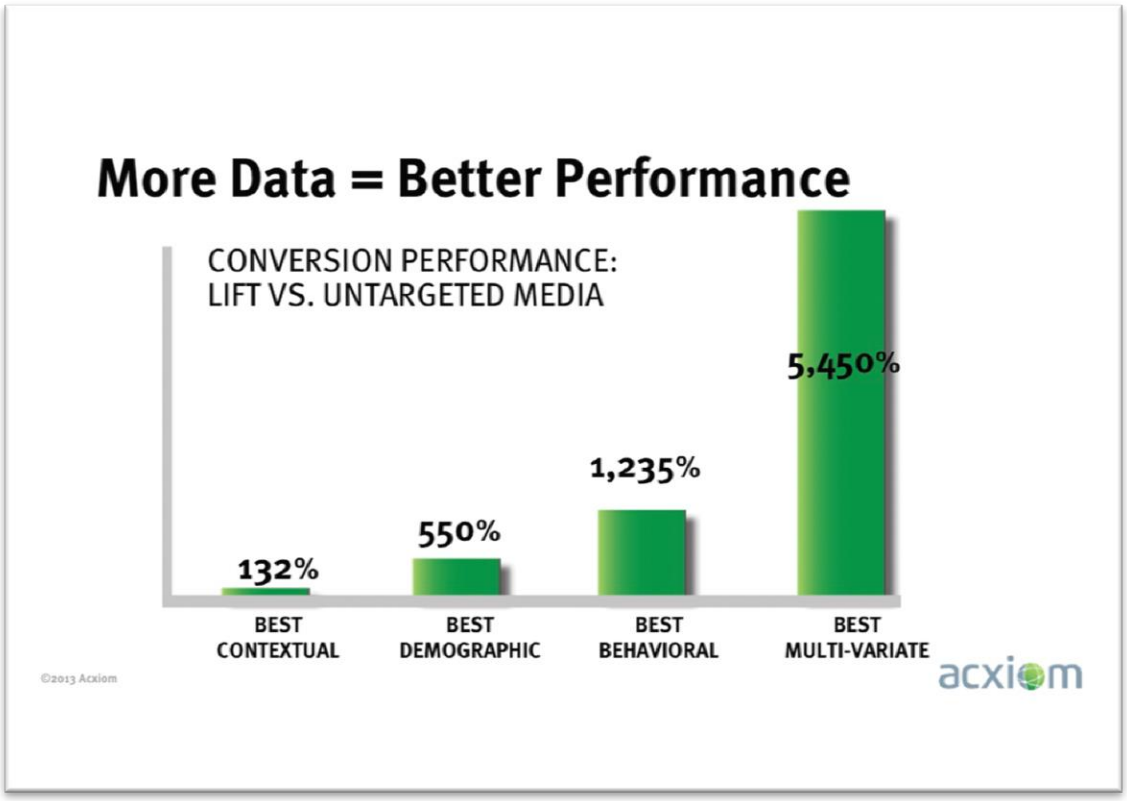
These examples illustrate the types of opportunity that will emerge for new organizations in the value chain to collect, aggregate and distribute customer data.

In some situations users will grant permission to an entity to gather data on their behalf. This opens up the possibility for data managers to operate as data repositories and guardians of an individual's data.

More data means more value

The economic rationale for combining data from multiple silos is powerfully illustrated by a product briefing from Acxiom[2]. Specifically, Acxiom illustrates the performance improvement from untargeted marketing to three single-strategy approaches – contextual targeting, demographic targeting and behavioral targeting.

Figure 3 Combining Data from Multiple Sources Significantly Improves Performance



Crucially, none of the individual strategies comes close to matching the performance of a multivariate approach.

When applied to an IoT scenario, the key insight from this example is akin to combining data across several single-purpose applications. The value that is created provides the basis for cross-application data brokers to emerge in the IoT eco-system.

[2] Acxiom is a US based customer data analytics company that provides business and market intelligence services. It claims to have a base of about 500m active consumer profiles.

Businesses, consumers and public-sector agencies will all benefit from IoT data sharing

Acxiom's experience is indicative of the many business benefits for IoT service providers from new data sources. In the case of consumers, there will be benefits in terms of new services. More data should also allow for a higher quality of individually tailored services.

Consumers as a group also stand to gain from wider societal benefits through services provided by public-sector agencies. This is possible when IoT data combinations are used to improve transport management for example. Specifically, sensor data from private vehicles, public modes of transport, roadway infrastructure (traffic lights, CCTV, environmental sensors, tool gates etc.) can be used to reduce transport congestion, to alert individuals with allergy and respiratory conditions, to help travelers to optimize their route and journey times. However, for this vision to be attainable, public sector agencies and individuals will have to be willing to share data about themselves and their connected devices.

Although by no means universal, there is at present a degree of consumer acceptance about the principle of sharing personal data. This is typically associated with sharing data in exchange for personal email (Google, Yahoo etc.), productivity and social networking tools that are provided at no monetary cost.

Consumers are also prepared to share data for services as in the case of shopping recommendations (Amazon and other e-tailers), advertising (retailer loyalty scheme or location-based) and professional networking (LinkedIn).

A common feature of all these 'free service' models is that consumers have no means to quantify the value of the data they are sharing. Their terms of trade are therefore opaque and not necessarily to their advantage. Contrast this to usage-based auto-insurance services, for example. Here, individual drivers choose to disclose defined attributes about their driving behaviors in exchange for quantifiable reductions in their insurance charges.

As the IoT market develops, the data shared by individuals, intentionally or inadvertently, will become more valuable. This is a direct consequence of the combinatorial power to generate better and more accurate personal insights from larger quantities of more granular measurements. However, the manner in which the value of IoT data will be shared more likely to favor the collectors - businesses and public authorities – over the providers in the form of individual consumers and their connected devices. Privacy principles are a means of ensuring that consumers are not placed at a competitive disadvantage while generating a framework of trust to encourage their longer term participation in valuable IoT services.

Privacy principles for the IoT future

Principles of privacy need to acknowledge the spectrum of consumer willingness to bargain away the data relating to themselves, the connected devices they own and third-party devices that they use. While the exposure of such data poses unknown risks with potentially harmful consequences it is equally important to acknowledge that there will also be benefits from service innovation.

The range of possibilities can be simplified into four scenarios as tabulated below which describes beneficial and harmful outcomes that may affect an individual either directly or indirectly.

	BENEFICIAL	HARMFUL
DIRECT IMPACT	In this case, an individual's data is used to provide a new service or to improve the quality of a service. The commercial basis may comprise a trade involving personal data for services provided. Within this scenario, it is also conceivable that an individual supplies data for direct, monetary gain e.g. by participating in a survey panel	Unauthorized use of data about an individual could be directly harmful and lead to an outcome such as identity theft. In terms of personal, connected devices tampering with a connected device could disable a home or car security system as a precursor to theft, for example
INDIRECT IMPACT	This situation corresponds to societal services in areas such as public healthcare, public transport systems and management of the environment. In this case, data for a population of inhabitants is used in aggregate form to improve the provision of health services (similar to the prediction of flu by analyzing search patterns on Google) or to improve transport efficiency, for example	This scenario applies to situations where a business offers a service to a consumer on the basis of third-party data about the consumer. The potential for a harmful outcome arises if the third-party data is false or inaccurate. Taken out of context such data could adversely affect the reputation of an individual. An illustration of this is data that jeopardizes an individual's credit score or incorrectly characterizes an individual's tastes or preferences.

Data privacy principles can alleviate concerns with the outcomes highlighted in these different scenarios.

- As the industry for IoT data matures, there should be an established set of principles and clarity about **data ownership** as well as the **terms of trade** that underpin the exchange of data, whether this is for services or monetary reward. Mechanisms to value data, similar to the principles that apply to frequent flyer and member rewards schemes, will help businesses and consumers to quantify their terms of trade. Such a development could be triggered if businesses and regulators determine that data records and profiles need to be valued and reported in company financial statements.

- In the case of indirectly beneficial data sharing, consumer trust will depend on **transparency of data appropriation**. In other words, the users of aggregated and anonymised data must be able to demonstrate that adequate safeguards are being applied in all aspects of the gathering, analytical and intervention processes surrounding public-good initiatives.

- In all scenarios, and especially the ones relating to harmful outcomes, individuals should have a right to **data accountability**. This would allow an individual to query a particular action from a service provider. For example, if an individual's credit score is lowered that individual should be able to find out the basis for this. Data accountability also applies in beneficial scenarios. If an individual receives a coupon to purchase a given product or service, it should be possible to query the logic for receiving the offer. Was the offer made on the basis of the individual's travel patterns, usage behavior as measured by a connected device or by because of being classified into

a certain group due to ownership of particular connected devices? This type of "track-back" capability is technically feasible as it lends itself to the rule- and classification-based approaches that are commonly employed in analyzing IoT data.

The goal of these principles is to empower users about the value of their data and to encourage their contribution of personal data to new IoT services. They form a basis for trust which should lead to a greater level of participation in the IoT economy.

The process of institutionalizing privacy principles will entail a significant effort in educating consumers and businesses about the benefits of IoT services, attendant risks and measures to protect their privacy rights and reputations.

The cost and complexity of implementing these privacy principles are not to be underestimated. Service providers in the IoT eco-system will need to deal with issues such as operational scale, granularity of data for accountability and monetization purposes, and jurisdictional obligations.

Privacy principles should nevertheless be viewed as a necessary investment to promote a well-functioning and trusted market. Such an approach will lower the incidence of companies "experimenting first and asking for forgiveness later" as this threatens the long term prospects and credibility of a highly promising sector. Rogue practices should not be allowed to ruin the benefits attainable by a responsible majority.

In conclusion, concrete action to promote privacy in the IoT market needs to take the form of:

- Consumer education initiatives about responsible management of personal data and associated measures of value.
- Development of industry guidelines about data ownership, data appropriation and data accountability.
- Promotion of privacy best practices for data management by businesses and public-sector agencies potentially involving the creation of a privacy-standards related brand or trademark.

---

more-with-mobile.com

more-with-mobile.com operates as a knowledge network and consultancy focused on the market for connected devices. It addresses emerging market segments, business model innovation and market development strategies.

This initiative was founded by Ken Figueredo who has been involved in market analysis and strategy assignments for organizations that are targeting new business opportunities in the connected products and services market. Ken is based in Washington D.C. and he can be reached at ken@more-with-mobile.com.