# TGF Impact of the Internet of Things

# Introduction

There is not yet an agreed definition of the Internet of Things (IoT), but the OASIS document “Transformational Government Framework e-Health Profile” Version 1.0 offers the following:-

*“a world where physical objects are seamlessly integrated into the information network, and where the physical objects can become active participants in business processes.*

*Note: Services are available to interact with these 'smart objects' over the Internet, query and change their state and any information associated with them, taking into account security and privacy issues.”*

This definition does not radically conflict with those offered by others and importantly includes the interaction with other systems and people who can use the information generated by a set of objects.

Such systems are already here and are being developed by a wide range of players across all sectors. Smartness is already being built into washing machines, TVs, refrigerators and other domestic products. These have various potential uses (and concomitant risks) and could use any of a number of connections within the home, to achieve local and possibly internet-level transmission needs.

The widespread and diverse adoption of these technologies and the ‘bottom up’ development that is necessary for the medium term development of the IoT are key characteristics that need to be considered and managed now as near-term projects start to build an infrastructure that would be prohibitively expensive to replace.

Some very large projects are already starting to emerge - often as Smart City initiatives. The full impact of the possible future extent of IT-based support can begin to be understood by considering the work going on in Japan to rebuild complete areas following the earthquake and tsunami in 2011*. [Provide some references to this work?]* There, the opportunity presented by the necessity for large scale reconstruction is being taken to introduce building and home management systems (amongst other innovations) to provide a sustainable environment that contributes to society and people’s lives. In this situation, they are, in most senses, starting from scratch and are able to agree and control the development of all systems. However, this is atypical and generally the development of a smart city or equivalent ecosystem will involve a number of organisations from a range of sectors who all need to work together and who also own existing services and systems that need to coexist and interoperate. In this scenario, building and home management systems will be fitted to new buildings and retrofitted to others.

However, further independently-supplied systems need to be able to leverage the capabilities that are already implemented. An example is an e-Health system that will contribute its own set of facilities but could usefully leverage home, building and city management systems in order to deliver its full potential. Without that capability, it would be necessary to implement much of those systems’ facilities within the e-Health system leading to duplication and increased cost.

Thus, the longer term should be considered by taking a holistic approach to all developments that involve IoT aspects. This paper identifies some areas where the emergent IoT and its application can impact programmes in which government organisations play a major part. It then goes on to relate these to existing TGF patterns that help government and partner organisations deliver programmes that contribute to the future rather than constraining it by delivering tomorrow’s legacy systems, today.

The broad areas that the IoT impacts include:-

* New partnership models
* Complexity for the customer
* Data Privacy
* Systems Management
* Network-related Issues
* Security and Resilience
* Sustainability

Each of these are introduced in turn.

# Possible Impacts of IoT-based Services.

# New Partnership Models

Services to a region or city as discussed above will need to be provided by a range of sectors and players within them. These will include government (all tiers), energy companies, transport authorities, health services, service companies, etc. as well as a range of suppliers to those organisations.

Many systems (e.g. weather and disaster management) are regional and cross government jurisdictions. Thus, federation between sectors and their services will become increasingly important in the medium to long term.

However, the IoT is being built bottom up with a range of standards (often specific to a sector) and network types.

The foundations for collaboration and orchestration within and across sectors need to be considered early on. Relationships may become very complex with a single organisation playing custodian, supplier and consumer roles within a service ecosystem.

Stakeholder organisations will all have their own objectives and channels to market and this provides them with a challenge. How do they manage their piece of the overall ecosystem and benefit from it whilst also contributing to the greater good of society at large?

Continuity of service over time is another issue that needs to be addressed in any service development as cessation of operations by any stakeholder for whatever reason would impact the overall service.

# Complexity for the Customer

IoT-based services can have many component parts and may be provided by consortia consisting of several stakeholder organisations. This complexity is bound to confuse all but the most digitally literate customers.

From the end-user (citizen or business) perspective, any multiplicity of players could give rise to several inter-related contracts and support mechanisms. Whilst variety, choice and competition are desirable market characteristics, straightforward customer access to a small number of (aggregated) systems and seamless support for them is a necessary prerequisite to service success.

Customers will wish to change suppliers. This needs to be as seamless as possible and not result in service interruptions as they will have come to depend upon the service and service interruptions could have potentially disastrous results.

**Data Privacy**

Data privacy is vital. Citizens and businesses need to trust the IoT and must understand the benefits that they gain in return for allowing aspects of their information to be shared.

On the supplier side, there is an understandable desire to leverage the information made available to them for service improvement and marketing purposes. This needs to be very transparent, to retain trust and be rigorously enforced to ensure good practice. Examples such as the recent NHS care.data situation in the UK and the general dislike by Facebook users of the new Facebook Messenger demonstrate the fragility of trust with citizens withholding assent and migration to a range of alternative messaging applications, respectively.

Such use of information needs to be transparent and not be hidden in long complex service agreements that virtually no one has the time to read, let alone understand.

The retention (and possible transfer) of raw information following a customer switching to an alternative supplier needs to be addressed in service agreements.

**Systems Management**

Many of the devices (and the data that they generate) will not be in the direct control or ownership of the public sector and the management of sensors and other devices within the community raises new challenges. Device failure or exhaustion of battery power might be mildly inconvenient in many cases but in others could be fatal (e.g. in an e-Health system). It is also important to recognise that services and the components within them will need to evolve over time.

Policies on asset management, monitoring, maintenance, upgrades, replacement, modification, status reporting, etc. of devices need to be open and available to all.

**Network-related Issues**

Network coverage may well be an issue. There is no single answer to connectivity and a range of alternative architectures might be needed to provide appropriate coverage for IoT and other services (sometimes even implementing several to serve the same location).

Different types of network (cabled, wireless, mobile or mesh) may be required depending on the service requirements (and more than one is likely to be necessary to support a single service – e.g. a cabled wireless backbone within a property). Some technical standards already differ for implementations within offices, industrial sites, homes, data centre and other uses.

Interference between systems (e.g. between home management systems in neighbouring properties), needs to be eradicated. This is not just a spectrum issue but could also occur at the application service level as these systems will need some level of configuration. This may be initially set up by a service provider but individuals will need to configure new devices as they subsequently acquire them. This raises the potential for accidental or malicious invasiveness into other systems.

**Security and Resilience**

Interference (discussed above) carries the risk of impacting the availability, performance or usability of a system.

Cybersecurity also needs to be considered. There have been localised malicious attacks on some home management systems but the threat increases exponentially in larger systems. The current issues with unsecured Wi-Fi connections will seem insignificant compared to (e.g.) interference with any element of an e-Health or power supply system.

**Sustainability**

The increased use of ICT to meet IoT objectives will have an impact on emissions and power usage. This may be positive but the impact needs to be understood.

Nig Greenaway

Fujitsu Fellow

15th September 2014