FUJITSU

Fujitsu response to Ofcom Call for Input: Promoting investment and innovation in the Internet of Things

Introduction

This call for input is timely, mentioning many areas of concern and coming at a time when some basic principles need to be laid down as the number of solutions being developed independently begins to mushroom. If left entirely up to individual initiatives, we could end up with a plethora of solutions that will impact the ability to achieve the possibilities that our economy demands from a Human Centric Intelligent Society.

Whilst bottom up innovation is both desirable and inevitable, if left completely unchecked, there is the potential for large investments to 'clash'. If relatively straightforward interoperability between solutions is not possible, we could reach a point where the unwanted complexities of duplication and incremental cost will mitigate against the benefits derived from the introduction of new solutions.

As an example, following the earthquake and tsunami in 2011 in Japan, Fujitsu has been working with others on the (re)development of the area using the latest technology, something that we would know here as "Smart Cities". The opportunity 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, a major supplier and its partners are, in some senses, starting from scratch and are able to agree and control the development of all operating 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 have existing services and systems that need to coexist and interoperate. More commonly, building and home management systems will be fitted to new buildings and retrofitted to others. Whilst competition needs to be encouraged to foster innovation and manage prices down, the lack of common standards and a concept of joint working (at the procurers end – i.e. between the transport, health and town planning level), is precluding many suppliers being willing to invest in this way.

In all the above cases, including the Japanese instance, further independently-supplied systems should 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 can usefully leverage the 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, basic frameworks and principles are a necessity now.

IoT Definition Application and Demand

In the medium to long term, federation between services will become more important. Many systems, for example weather and disaster management, are regional and span across government jurisdictions. Services for a society will be delivered by a range of sectors including government (all tiers), energy companies, transport authorities, health services, service companies, etc. as well as a range of suppliers to those organisations.

However, currently the devices and systems relating to the IoT are being built bottom up with a range of standards (often specific to a sector) and network types. As such, in order to ensure the UK takes full advantage of the potential of IoT technology, it is necessary for the foundations for collaboration and orchestration within and across sectors to be laid now whilst still allowing innovation and competition within sectors. Ofcom is in a unique position to inform these policies and support their implementation and evolution.

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 pie and benefit from it whilst also contributing to the greater good of society at large?

From the end-user (citizen or business) perspective, this multiplicity of players can cause confusion, multiple contracts etc. and whilst variety, choice and competition are desirable, straightforward customer access to a small number of aggregated systems and seamless support for them is a necessary prerequisite to success – as is joined up procurement to maximise the return on investment from suppliers.

Early engagement by Ofcom in guiding the development of IoT systems will be of significant benefit to both organisations providing such services and end-users, standardising outputs and minimising the number of applications needed to be used.

Spectrum Requirements

Flexible spectrum management approaches will be crucial to enable IoT solutions that can deliver quality, predictability and security for businesses and consumers. The harmonisation of spectrum to respond to increasing data demands generated by IoT is another key success factor to reach the necessary economies of scale in terms of both network equipment and devices.

Some network operators have proposals in this area but claim to have few people at UK or European level that they can address them to. Hopefully, Ofcom will already know of these requirements, or be able to gather them as part of this current exercise, and be in a position to develop them into a strategic approach that can be shared with industry and internationally.

Network-related Issues

With the introduction of such a wide range of new services, coverage is always likely to be an issue. As with broadband provision, there is no single answer and a range of alternative architectures will be needed to provide appropriate coverage for IoT services, sometimes even implementing several to serve the same location.

Different types of network, such as cabled, mesh, mobile and wireless, will be required depending on the service. More than one is likely to be necessary to support a single service, for example a cabled wireless backbone within a property. Some standards already differ for implementations within offices, industrial sites, homes, data centre and other uses. With some cabled parts of networks being built into properties, this IoT 'infrastructure' may well need to be reflected in building regulations. There is initially a role for Ofcom here to ensure that standards are set in a way to best support efficient development of IoT in the UK.

A particular issue around networks is likely to be that of interference between similar systems, for example home management systems in neighbouring properties. 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 initially be 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.

Ofcom is uniquely placed to develop a framework for IoT network provision and oversee its adoption by the full range of service providers.

Security and Resilience

IoT devices will increasingly become essential to the correct functioning of infrastructure – for example, cities, buildings, transport – with expected serviceable life-times of many years, if not decades. If the capabilities of ICT continue to follow historic trends, improvements by a factor anything between 10 and 100 are possible over the next decade. Such improvements will be available to cyber-criminals and cyber-terrorists.

Cyber security therefore is a likely to be a significant consideration for the IoT devices. There have already been localised malicious attacks on some home management systems, however the threat

increases exponentially as we implement bigger and bigger systems which communicate with each other. The current issues with unsecured Wi-Fi connections will seem insignificant compared to potential interference with any element of an e-Health or power supply system for example.

The ability to update devices incorporated into infrastructure – e.g. vulnerability remediation, key refresh (including longer keys) and additional security measures – throughout their lifetimes, is therefore essential to mitigate the risk that infrastructure becomes vulnerable to overwhelmingly more capable attackers. Worryingly, it is noted that in the UK "smart meters" are already being rolled out that have no capability for remote software updates.

This is not a new challenge, as years of SCADA problems illustrate, but the increasing pervasiveness of, and dependence on remote control and monitoring make regulating standards for such IoT devices essential. This may mean that elements of the IoT will come to be defined as Critical National Infrastructure. Nor is this threat confined to commercial or publicly operated infrastructure: an actor with the ability to launch a simultaneous attack on large numbers of consumer devices, for example smart home control devices, could also wreak havoc to services such as utility provision.

The availability of systems on a single chip (SoCs) incorporating 3G/4G mobile telephony connectivity makes possible consumer IoT devices which are connected directly to mobile telephony networks. Such devices, whose designs will invariably be driven by sales price competitiveness, are prone to have security vulnerabilities, similarly to most broadband modems, but inadequate provision for firmware updates. Especially at the cheaper end of the market these devices will be sold "as seen" with minimal, if any, after-sales support. It is strongly recommended that devices that do not of themselves have provision for through-life security management not be permitted to connect directly to mobile networks, but rather through a local "gateway", for example a home hub or mobile device, which does have such provision.

As such, methods should be explored as to how to effectively ensure the secure transmission of data between devices. There are a variety of ways in which this can be achieved. A consideration to be made is that whilst there will be a massive number of devices connected to the IoT, the sensitivity of data from each is likely to depend on who needs to access that data, what they want to do with it and what would happen if they weren't able to do so. The vulnerabilities therefore may not be in the existence of the data on the IoT so much as who is using it and for what purpose. Furthermore, data transmitted by each IoT device is likely to be very small and does not necessarily have to carry any contextual data. The more contextual data that accompanies the status data, the more valuable and vulnerable the data will be to exploitation by an attacker. If a system could be devised which allows individual users or organisations to create their own IoT models of what they depend upon but keep those models inside their protected environments. The data transmitted to and from the IoT will not in itself offer intelligence to an attacker.

Obscuring the contextual information from IoT data will therefore allow the transmission of sensitive data without giving intelligence to an attacker. Obfuscation methods are likely to be able to achieve such a result. For example, renaming identifiers and removing debugging information in Java code can hide the intended meaning of communication and make it harder to interpret.

Ofcom will need to introduce, maintain and enforce a good practice framework across all service providers and stakeholders.

Data Privacy

IoT devices are predicted to be rolled out on a scale (e.g. trillions) and at a pace that is truly daunting. The volumes of data generated by these devices, from increasingly diverse sources, and the ubiquitous processing of that data in ways never envisaged by current data protection legislation will have serious implications for privacy. 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. Commercial success of IoT initiatives depends crucially on the trust of owners and users that devices will communicate only that data and perform only those actions to which they have consented.

Whilst 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. Recent examples such as the 'care.data' situation and the dislike by many Facebook users of the new Facebook messenger service demonstrate the fragility of trust with citizens withholding assent and migration to a range of alternative messaging applications, respectively. Mobile and home entertainment systems have also been known to collect unauthorised data from their users. Ofcom needs to work with the Information Commissioner's Office in this area.

As services beyond those offered by vendors of single domestic appliances and devices become available, Ofcom could develop and enforce a framework to address these service-level concerns. This is suggested as an initial step and experience may generate extension downwards as organisations seek to further leverage information that can affect individuals - e.g. the ability to set insurance premiums based upon driving habits is likely to be seen as innocuous by many but when this is incorporated with other information sources might be perceived as being too invasive and having undesirable side effects.

To address these concerns an additional set of Data Protection principles is likely to be needed for the IoT, not least because of the role played by devices which are owned or operated by data subjects. A sample set of principles is given below:

- A device must only act or communicate for a particular purpose on the authority (or consent) of an individual or entity. The individual or entity must have the legal right to withdraw their authority.
- The purpose(s) for which a device may act or communicate must only be those authorised by the individual or entity on whose authority it does so and who has been fully informed of the purpose(s) and of the information that the device will communicate.
- A device may have multiple identities, depending on the context or purpose for which it is being used. Some identities may be asserted by the manufacturer, provider or operator of the device; other identities may be specified by the owner or user of the device (who authorises the use of that identity for the current purpose). In all cases, each identity needs to be sufficiently assured for the purpose for which it is being used. (It should be assumed that a relying party will make a judgement on whether the identity is sufficiently assured.) Multiple identities reduce the ability to associate the identities of devices with the identities of people.
- The data communicated by a device to any third party must be the minimum required to achieve the authorised purpose.
- The individual or entity who authorises a device to communicate personal data to a 3rd party must have the right to be provided, on request, with copies of all of the personal data thus communicated. The individual or entity must also have the right for inaccurate data held by a 3rd party to be corrected.
- There needs to be a procedure whereby individuals or entities can seek independent resolution of any dispute arising from interpretation or application of the principles above.
- Finally, there must be provision for exceptional circumstances, with an onus to show that the proposed action is proportionate, and subject to independent oversight,

Note that these principles apply equally to sensors, virtual things (aka agents) as to physical devices.

For further information a BCS paper, Internet of Things Working Group: Report to PPAB1, discusses the potential to use and abuse the IoT and discusses the application of Data Privacy Principles to the IoT.

[1] http://www.bcs.org/upload/pdf/iot-report-jun13.pdf

Numbering and Addressing

Whilst devices need to be addressable, those addresses should be transferable or able to be changed to enable customers to switch suppliers. This raises further security issues.

The vast range of devices that will be connected to the IoT means that an approach to device management needs to be considered. Suppliers and service providers should look to address this by means of a risk-based approach and the resultant risk registers should then be published. Device failure or exhaustion of battery power might be mildly inconvenient in many cases but in others may be fatal, for example in an e-Health system. It will be necessary for suppliers to introduce appropriate policies on monitoring, maintenance, upgrades, replacement, modification, status reporting, etc. of devices. These should be open and legally available to all.

Digital Literacy

IoT services can have many components and may be provided by consortia consisting of several stakeholder organisations. This complexity is bound to confuse all but the most digitally literate customers and services should be offered via a well-defined service interface. This needs to pay specific attention to security and privacy concerns of the customer.

Freeview-style retuning exercises are not acceptable in IoT scenarios as the customer is very unlikely to be capable of managing it and the multi-stakeholder/collaborating services model does not readily lend itself to engineer support for such exercises.

The successful development of IoT will require a competitive market, where suppliers are able to innovate and attract customers. Therefore an important factor in IoT services is that it should be possible for customers to change suppliers of services. This needs to be as seamless as possible for multiple reasons. Firstly, changes should not result in service interruptions, as following the development of a comprehensive IoT infrastructure customers will have come to depend upon services provided through the IoT and interruptions could have disastrous results. Furthermore, the simple switching of service providers will be necessary so as encourage competition, similarly to those initiatives pursued within the energy and banking sectors.

Digital literacy will also be necessary for security reasons. With the expected massive increase in IoT devices in the next few decades, it will be necessary for people to have the ability to understand and interact with the systems that run in their household, both to ensure that they can obtain the most use from them, but also to protect them from intrusion. Whilst basic manuals with each device can provide some measure of instruction in how to use devices, a broader level of digital literacy in the general population will be necessary. This is particularly of concern amongst older age groups that already disproportionately suffer from digital exclusion. A failure to address this will mean that those who could most benefit from IoT services cannot take full advantage of them.

Data Analysis and Exploitation

Such use of information needs to be transparent (and not hidden in long complex service agreements that virtually no one has the time to read, let alone understand). See the earlier comments on privacy and trust.

The retention (and possible transfer) of raw information following a customer switching to an alternative supplier needs to be addressed in service agreements and by ICO-managed processes (that presumably already exist).

International Developments

IoT services are already being pursued around the globe. As mentioned above, Fujitsu already has extensive experience of developing integrated IoT systems for entire cities in Japan. On a smaller scale, 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. Suppliers of these devices seldom have any desire to increase their costs by providing multiple connectors and thus collectively employ a range of solutions that tend towards the entropy mentioned in the IoT Definition Application and Demand section.

As such there is an opportunity for Ofcom to work with its counterparts in other countries (especially those in the US and the Far East) to agree standard connection types for families of devices to minimise this divergence and help to generate a common approach and, in the longer term, common platforms.

Ofcom should also liaise with other countries to address spectrum and other network concerns. As part of this, UK solutions such as HyperCat can be promoted and (even if UK solutions are not adopted) should lead towards a degree of convergence. Such activities should facilitate the UK export of solutions and expertise.

Ofcom's Role

Ofcom does need to use its position and influence to raise the issues brought by the IoT and where possible be more proactive in standards setting. However, it needs to take care to not over-mandate the solution stack and to leave room for innovation and collaboration between large and small players in the market.

The increased use of ICT to meet IoT objectives will have a Green impact and Ofcom needs to work with other bodies to address the sustainability aspects.

The complexity of many IoT projects means that effective governance is vital. Standards organisations are starting to address this area and some papers Fujitsu staff have contributed to are publically available:
PAS 181:2014 Smart city framework. Guide to establishing strategies for smart cities and communities by BSI
TGF eHealth Profile CN01 by OASIS

Both of these papers are based on the OASIS Transformational Government Framework Version 2.0

Ofcom might like to review these (and others that are currently in development) and promote their adoption by IoT projects.