Response to Ofcom Consultation: Promoting Investment and Innovation in the IoT

Weightless SIG, August 2014

Introduction

The Weightless SIG is a not-for-profit standards body which has developed an open standard for IoT communications enabling low-cost devices to communicate over wide-area networks with a battery life of up to ten years.

Our responses to the topic areas highlighted by Ofcom are provided below.

IoT definition, applications and demand

The range of IoT devices, applications and supporting services that is likely to emerge across different industry sectors, along with views on potential market size. We are particularly interested in stakeholders' definitions of the IoT and views on which applications are likely to dominate and the characteristics of these applications (in terms of their range, quality of service, connection speed and data throughput, radio cost, battery life etc.).

Weightless is intended to be a general-purpose IoT standard which is suitable for the widest range of applications. As a result, we do not tend to focus on specific applications nor provide market forecasts. Our view is that this early stage is somewhat akin to the launch of the Apple Apps Store – while some applications can be predicted it is just not possible to understand the breadth of what will eventually materialise. As a result, seeking to understand applications in too much detail may well be counter-productive, instead Ofcom should focus on a framework that is as flexible as possible to allow for the maximum innovation.

However, it is worth considering which might be the first applications. This is because it is important to get the market conditions right to facilitate the emergence of those applications which will lead to an IoT infrastructure being deployed and subsequent growth. Our view is that these are likely to include:

- Industrial productivity. This includes applications such as oil refineries and water treatment plants which have dispersed sensors and actuators and where remote monitoring and control can bring clear productivity benefits. We have already seen significant interest from the water, oil and gas industries.
- Smart cities. These have the benefit of ease of covering a relatively small area and potential for a large number of applications such as smart parking, street lighting, smart dustbins and traffic management. Also, the large number of smart city demonstrator projects will tend to drive deployment and application development.

- Smart metering. Many countries, including the UK, have a defined smart metering programme which can drive IoT deployment, although unfortunately in some cases technologies have been selected which are single-purpose or ill-suited for wider IoT usage.

Providing particular support to some of these applications might enable more rapid IoT emergence than would otherwise be the case.

Spectrum requirements

The need for additional spectrum to meet the expected demand for wireless connections between IoT devices. In particular, we would welcome views on which specific frequency bands are desirable, the need for internationally harmonised bands, whether additional spectrum should be made available on a licensed or licence exempt basis, and whether shared or dedicated spectrum bands will be needed.

All wireless communications requires spectrum. Our view is that existing wireless systems, such as cellular solutions, are not well-suited to the majority of IoT applications due to their relatively high cost and insufficient battery life. Hence, we believe that a new wireless solution needs to be deployed to deliver the full promise of the IoT.

We believe that ideally spectrum for IoT applications should have the following characteristics:

1. Below approximately 1GHz to facilitate long battery life by enabling long range with low transmit power.
2. Sufficiently plentiful to allow the use of range extension techniques such as spreading, we prefer at least 20MHz of spectrum (to allow 5MHz channels with a repeat pattern of 4) but note that it is possible to work with less, such as 1MHz channels, especially in the early deployments where the number of devices is relatively low. More spectrum would be desirable to enable competing systems and increased capacity where needed.
3. Globally harmonised, or at least have the potential for global harmonisation, as only globally harmonised solutions achieve the economies of scale and market acceptance needed to be successful.
4. Available in a timely and low-cost manner, remembering that for emerging areas auctions are problematic – for example the first cellular licences were given out rather than auctioned.

While it would be ideal if spectrum fitting this description were made available on an exclusive basis for IoT, we are alive to the lack of spectrum below 1GHz, its value and the demand from competing organisations. We therefore believe it is more practical to anticipate shared access and have designed Weightless to operate effectively within shared spectrum. More specifically, our preference to fulfil all of these requirements is TV white space although we are currently concerned by the lack of progress on these bands outside of the US and UK. Hence, our current intent to deploy Weightless in other bands such as 868MHz until there is wider global availability of white space or other unlicensed frequencies that fit the criteria set out above.

Within any unlicensed bands adopted we would prefer some certainty of access. This would enable Weightless networks to more credibly offer QoS guarantees to those users that require it. For example, part of the TV white space or 868MHz band could be reserved for IoT solutions or there

could be channels set aside for applications that were seen as being socially beneficial such as health-care. With a database approach many different variants of this sort could be envisaged and indeed, access could be changed over time as demand became clearer. Equally, Weightless has excellent support for a range of QoS requirements and can both avoid interference and prioritise traffic. Hence, even without any form of priority access we believe it can provide solutions suitable for the vast majority of applications.

There has been much debate about whether operators will deploy networks in unlicensed spectrum and whether QoS can be offered. We believe that such deployments can occur – for example there are proprietary IoT networks being deployed in unlicensed spectrum and operators have deployed Wi-Fi-based networks for many years. Indeed, today's cellular networks are so reliant on Wi-Fi offload to function that it could be said that cellular networks are as much based on unlicensed spectrum as they are licensed. Congestion issues in unlicensed spectrum typically build very slowly over time allowing network engineering to be applied to add additional capacity or resilience. Congestion can also occur in networks in licensed spectrum as we have frequently seen with cellular networks. Finally, unlicensed spectrum does not require the payment of an auction fee, leaving the operator with a strong business case able to "insure" against future growth in use of the band.

In the longer term – five to ten years perhaps – it may be that operators of IoT networks will have a stronger business case and may seek to move to licensed bands. For example, they might purchase spectrum at 700MHz were this to be auctioned in due course.

Network-related issues

We are interested in views on a number of IoT network and infrastructure related issues, including:

- *Approaches to delivering IoT services: Broadly, services could either be delivered using conventional mobile networks, in general licence exempt bands or via bespoke networks that are optimised for the IoT. Other approaches may exist between this range of options. We are interested in opinions on the approaches to delivering IoT services that will likely emerge, citing advantages, disadvantages and views on which applications might be better suited to a particular approach.*
- *Degree of openness: IoT services could be deployed over entirely open networks, i.e. any manufacturer's device conforming to a particular technical standard can be connected; or over a closed network, in which the operator controls which devices can access the network. We are interested in views on which of these (or similar) approaches might develop, whether particular services are suited to an approach and what the implications might be for the development of the IoT. We are also interested in views on the role of open versus proprietary standards.*

We do not believe that cellular networks are suited to the bulk of IoT applications. This is because:

- Chipset costs are generally too high, especially for 3G and 4G networks and factors such as royalty payments tend to limit the scope for cost reduction.
- Battery life is insufficient.

- Coverage is insufficient – for example the solution proposed for smart metering in the UK using GPRS is unable to reach the required coverage levels and so ancillary technologies such as mesh are being "bolted on".
- Message sizes are too large. For a GPRS-based solution we estimate that often 400 bytes of data are sent in the process of waking up, moving from passive to active, acquiring an IP address, sending signalling information, sending data and then going through the reverse process. For many IoT applications message sizes are 4 bytes or less, and hence there can be a 100-fold overhead associated with using cellular. This is inefficient and appears unsustainable without large-scale specification change.
- Numbering issues are problematic.
- SIM cards are inappropriate and add cost. Machines, after all, are not subscribers and have no need for a SIM card.

There are also problems associated with the incompatibility of the business model for IoT with that for cellular that makes it difficult for cellular network operators to optimise their networks in the way needed to drive IoT costs down.

Our observation on open standards is that all of the wireless technologies we routinely use today are open standards. History suggests that proprietary wireless technologies do not succeed for well known reasons such as lack of competition, concerns over monopoly supply and limited scope for innovation. We see no reason for these drivers to be any different in the IoT and hence are convinced that only open standards will succeed.

We are less clear about open and closed networks. We believe that the majority of IoT applications are best enabled by an open network, akin to a cellular solution, which shares the network cost across many users and provides higher levels of coverage and functionality than any one user group could typically afford. However, there may be some applications, such as on an oil refinery, where provision of coverage is inexpensive and the owner prefers the additional level of control that deploying their own network provides. Operating in unlicensed spectrum is advantageous in allowing both of these deployment modes to exist side-by-side.

Security and resilience

Across the range of IoT services there are likely to be a variety of security and resilience requirements. At one extreme there may be applications that can be supported on a best efforts basis, whereas other applications may need to be highly available and resistant to malicious attack. We are interested in views on the steps required to enable the IoT to support high levels of security and resilience.

We see security as critical. IoT networks will be subject to various attacks and must be robust against them. This requires both strong encryption but also two-way authentication (the device authenticates the network and the network authenticates the device). Security considerations for the IoT can be different from cellular. For example, messages are often short and repetitive – a reading from a smart meter may only differ in the lower digits changing from reading to reading. This is challenging cryptographically, with solutions needed that randomise data first, but yet add very

little overhead to the message size. For some applications authentication of the network by the device is essential otherwise the device could “park” on a rogue network and never move off, unlike a cellular system where the subscriber might quickly appreciate they were not getting a service they recognised. For this reason, Weightless specifies an industry-standard 128-bit AES-based encryption and authentication approach that, to our knowledge, has never been compromised.

Security of the data once decrypted and stored in a central server or database will also be critical but is beyond the scope of the Weightless standard.

Resilience against attack is mostly inherent in having a secure approach. However, some attacks such as jamming cannot be avoided with security. Within Weightless we use intelligent frequency hopping to work around jammed frequencies. The use of white space makes jamming across the entire band difficult and readily detected since it would compromise TV reception.

Even for those applications that appear to have little need for security we believe it is important that security is applied. This is because stories about being able to “hack” into such devices, even if irrelevant, could lead to a perception of general insecurity across other applications.

Data privacy

We are interested in the nature of privacy and data protection issues that may arise through the development of the IoT, including views on approaches to appropriately manage personal or commercially-sensitive data.

Privacy is critical. If there is a perception that privacy is being compromised or is unclear it could set back the deployment of the IoT by many years. However, privacy needs to be handled on an application-by-application basis. For example, there may be some applications where openness is needed such as temperature sensors scattered around a city. There will be some, where privacy is fundamental, such as healthcare. And there will be those in between such as smart dustbins, where individual data may be private but aggregate data may be public.

We believe that privacy needs to be addressed on a case-by-case basis, with great care and sensitivity.

Numbering and addressing

We are interested in views on the likely nature of demand for device addresses and to what extent this demand might be for electronic addresses and/or telephone numbers. We are also interested in the extent to which demand for device addresses, in the form of telephone numbers, IP addresses or other identifiers, could be a barrier to the deployment of IoT services.

Numbering is an issue that requires some care. For example, 128bit IP addresses could be much larger than the message payload adding unnecessary overhead. Equally, we see no strong reason why devices need to conform to existing numbering schemes. For that reason, Weightless uses its

own internal numbering system, with translation to other approaches such as IPv6 at gateways as necessary.

Devices

We would welcome stakeholders' views on technical and commercial developments that could affect the cost and capability of IoT devices, in particular in relation enabling the manufacture of low cost devices with low energy consumption and long battery life. We are also interested in views on the role that existing or emerging device operating systems will play.

All the technologies needed to enable low cost and long battery life already exist today and have been demonstrated. We would expect the normal "Moore's Law" progress to result in ever-lower device costs over time. We do not believe devices should have an "operating system" as such – this imposes an extra burden in terms of processing requirements and power consumption.

Digital literacy

We welcome views on the role of digital literacy in underpinning the growth in take-up of IoT devices. What steps, if any, will be required to enable citizens and consumers to understand the potential benefits and risks of the data created by their devices being shared? What steps is industry taking to address this challenge?

As with privacy it seems likely that this will need to be handled on a case-by-case basis and is probably best undertaken by organisations responsible for the "vertical" segment, such as eg the Continua standards body in the healthcare arena.

Data analysis and exploitation

The capture, analysis and exploitation of "big data" from multiple devices and applications to provide new, innovative services. We are interested in views on whether there will likely be demand for such services, on the nature of the services and whether there are any barriers to their development.

Weightless is broadly not concerned with how the data is used. However, it may be better to collect and manage data in "silos" initially and only consider big data analysis once the issues and concerns associated with the silo approach are well understood and solved.

International developments

In the longer term, IoT equipment is likely to be developed for a regional or global market; this will be necessary to drive down device costs and achieve economies of scale. We welcome views on relevant international activities, such as the development of common technical standards, trials and commercial deployments.

We believe that, just like Bluetooth, a single global standard will emerge for IoT connectivity. Standards like Weightless are inherently global in nature.

The use of dynamic spectrum access is one of the many options for providing spectrum for connecting IoT devices. We recognise the contribution that Ofcom has made in white space studies in many regulatory and standards organisations, including ETSI and CEPT. This initiative has assisted in the preparation of several ECC Reports and the ETSI harmonised white space standard, and continues with significant inputs to the current CEPT work on a regulatory framework report.

Weightless views this work as essential to ensure spectrum harmonisation for white space devices that will enable market potential for UK industry to reach European and international markets.

We therefore encourage Ofcom to continue to provide resources for its European and international work on radio spectrum regulation, of which the IoT is just one application.

Ofcom's role

We recognise that the IoT is a fast-moving area in which industry is well-placed to create a range of innovative technologies and services. To enable us to best support these efforts, we welcome stakeholders' views on our role across the range of policy issues raised in this document, including spectrum management, network resilience and security.

We broadly agree with Ofcom's view that much of the progress in the IoT area is best left to industry. The clear exception is spectrum. Setting aside spectrum for IoT (even if it is shared with a primary user, such as white space) would both be an enabler and make it clear that Ofcom supported this application and is likely to continue to do so in the future. Working internationally to ensure appropriate standards and encourage other regulators to harmonise the same spectrum is also of great importance.