Program Planning Professionals Ltd - Response to OFCOM Consultation on IoT

Summary

Program Planning Professionals Ltd believes that the UK in general and Ofcom in particular has the opportunity to take leadership in this field. It forms a key part of the "deep fibre" strategy we advocated in our response to the DCIS Consultation on Infrastructure, and many of the concepts we advocated there are relevant here too.

Just some of the important issues we can already see emerging in this domain include standardisation, competition, addressing, data protection, security, spectrum availability, price – and demand. Early "in-home" applications are already emerging… but there are such a huge range of possible uses far outside the home that must also be considered to enable a "holistic" and inclusive regulatory strategy can be formulated. We also note that Ofcom may have insufficient resources to promote innovation and investment without assistance.

Our Responses go into more detail on these and related matters and are set out below:

OFCOM Questions

1.46 ***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.).*

There are many slightly differing definitions of the IoT. A simple definition is below:

> "The IoT can be defined as any embedded devices that have connectivity, directly or indirectly, to the Internet. A key element is that IoT will focus on receiving and transmitting data without any human intervention."

The more comprehensive explanation we favour comes from (http://whatis.techtarget.com/definition/Internet-of-Things):

> "The Internet of Things (IoT) is a scenario in which objects, animals or people are provided with unique identifiers, and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. IoT has evolved from the convergence of wireless technologies, micro-electromechanical systems (MEMS) and the Internet.
>
> A thing, in the Internet of Things, can be a person with a heart monitor implant, a farm animal with a biochip transponder, an automobile that has built-in sensors to alert the driver when tire pressure is low -- or any other natural or man-made object that can be assigned an IP address and provided with the ability to transfer data over a network. So far, the Internet of Things has been most closely

> associated with machine-to-machine (M2M) communication in manufacturing and power, oil and gas utilities. Products built with M2M communication capabilities are often referred to as being *smart."*

The form that IoT *applications* will take will be heavily influenced by whether or not we favour and promote IPv6 deployment as the basis for all IoT applications, because it is Ipv6 which enables us to give unique identifiers to all "things" on the planet – multiple times – and thereby unleash the full potential of IoT applications.

Kevin Ashton, cofounder and executive director of the Auto-ID Centre at MIT, explains the potential of the Internet of Things thus:

> "Today computers -- and, therefore, the Internet -- are almost wholly dependent on human beings for information. Nearly all of the roughly 50 petabytes (a petabyte is 1,024terabytes) of data available on the Internet were first captured and created by human beings by typing, pressing a record button, taking a digital picture or scanning a bar code.
>
> The problem is, people have limited time, attention and accuracy -- all of which means they are not very good at capturing data about things in the real world. If we had computers that knew everything there was to know about things -- using data they gathered without any help from us -- we would be able to track and count everything and greatly reduce waste, loss and cost. We would know when things needed replacing, repairing or recalling and whether they were fresh or past their best."

Machines are already collecting and transmitting such data, with (and sometimes without) informed consent, and the number of potential applications is vast. It is all happening regardless, and it is a genie that cannot be placed back into the bottle. The implications of such a fundamental change are so huge that Ofcom alone given its resources and limited powers will only be able to play a minor, but nonetheless hugely important, role in what happens next.

The consultation at 1.1 sets out a range of possible applications in the healthcare, transport, and energy sectors. To this we would recommend adding the *environmental* sector. Sensors to detect water quality, earthquake risk and floods are already in use, and are of considerable help to "first responders" in assessing how best to prioritise during emergencies.

The key factor in our view is to give due consideration to what the IoT and big data makes possible – predictive analytics – rather than to seek to formulate a list of possible applications at this early stage in its development when it will be necessarily incomplete. This could be applied in some way or another to almost *any* field in some form or another. This makes assessing the market size virtually impossible.

At this stage in the IOT's development we think that a critical success factor will be the mass availability of cheap and highly reliable sensors which can last for a long time, consume little power, and still provide some security by design at their inception. They will probably be capable of transmitting small volumes of data over long distances, as mass data collection will be taking place "upstream" so they will not need to. This approach would, we believe, lead to the most rapid uptake, provided it was accompanied with the active promotion by

Ofcom of open standards for such devices (called “constrained devices”) to prevent customer lockout and to keep end pricing low. More recently most development had not focused on the needs of such devices. If one also accepts the inevitability of “deep fibre” then a key focus needs to be finding suitable spectrum to interconnect with such a backbone cheaply and robustly. We turn to spectrum issues next.

1.47 ***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.*

The IoT already exists in “proto form” and already makes use of all kinds of spectrum. Perhaps the most well-known issues include:

- Bluetooth LE (this is the modified form)
- 802.15.4 (for home and building applications, offering LAN functionality)

However lower frequencies will be needed for cheaper WAN applications – as well as higher ones. It should always be remembered that the devices themselves don’t care what spectrum is used – so long as they can use it in the way they want to and when they want to.

Due to the laws of physics and state of technological development, the lower reaches of the spectrum are heavily congested, but ideal for transmitting smaller amounts of data over long distances. However, the spectrum most likely to be readily available is high frequency high capacity, but suitable nonetheless for short range interconnection.

The logical next step would be to await the outcome of WRC-15 because it is already too late to influence it in any meaningful way. Once we know what the internationally harmonised available bands are and whether use in the band is primary or not we can then base a longer term strategic approach to spectrum on this information. Spectrum below 2.4GHz will certainly ideally be needed – but might well not be available unless on a shared basis. Dynamic shared access could well assist greatly because it is now possible for devices to manage in such an environment.

Therefore wherever possible Ofcom should seek to use unlicensed spectrum, save where the risk of harmful interference, mission criticality or security requirements make it essential to licence. Licensing puts prices up

We conclude this section by adding that setting aside spectrum in the 700MHz guard band would not be appropriate. There is already considerable conflict in the band and litigation is a real possibility (resulting to serious delay to IoT deployments relying on it). Part of the guard band would also be a possible home for Programme Making and Special Events (“PMSE”) users, sharing with Broadband ESMCP users because the proposed commercial network based ESMCP solution is undeployable for multiple reasons. A direction to Ofcom on this matter can realistically be anticipated.

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

1.48.1 ***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.*

Conventional networks were simply never designed to deliver IoT type functionality. Though they could, IP to the edge over IPv6 makes more long term sense and can cope with the huge numbers of additional devices that will need to be able to communicate. This approach helps to defines in turn in which standards Ofcom should be tracking closely.

The advantages and disadvantages of licensed (security, availability, planning, no interference, but at a price) over unlicensed spectrum are broadly the same in this domain as in others. However strategically we should consider whether or not we will be continuing in the UK with spectrum pricing in the longer term. We set out in detail in the response to the DCIS Infrastructure why this could well happen. Many IoT companies will not necessarily be huge multinationals yet they might well be the source of fantastic and innovative services. A hybrid allocation system similar to that used in France might really help kick start the IoT in UK.

1.48.2 ***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.*

Maximum consumer welfare benefits are typically achieved by the use of open standards whenever possible. Ofcom has duties under Section 3 of the Communications Act already in this regard. Closed networks do have a role when high security and robustness is required.

It is important that we not be tied for IoT growth just to mobile networks – even they would not want this. The IoT is far bigger in its potential impact and should not be constrained by using yesterday's technical solutions to address tomorrow's problems. This is NOT to say the mobile networks have no role – quite the opposite. They bring very useful skills and experience – but the business model for IoT applications is different, the spectrum

requirements will vary, and the promotion of competition is a statutory duty on Ofcom already and therefore must be respected.

1.49 ***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 were somewhat surprised to note in the recent DCIS consultation that infrastructure security and authentication played no part in what was otherwise a comprehensive consultation document. In facte do not recall a single mention of them. Nevertheless we feel that it is of *critical importance*, and wherever possible must be designed in at the start.

Security has to be considered "holistically" from the network, to the devices to the chips themselves – as well the services likely to be operated and what characteristics and need for security (including a statutory requirement for data security coming from the proposed new EU Data Protection Regulation) they have. This makes the question incredibly complex and worthy of a consultancy study in its own right (which we would be delighted to undertake!). What we therefore do here is to focus on areas where Ofcom can have an impact, for its impact on devices or chip design for example can at best only be marginal.

We refer earlier in this response to "constrained devices," and will focus on the impact such devices could have on security and resilience by addressing the key standards, their aims, and what impact this might have.

A key consideration is that 802.15.4 networks (so called "constrained networks") work with smaller packet sizes and lower bandwidths. IPv6 has the capability to give every device a unique address but the protocol overhead required is simply too great. IETF's "6LoWPAN" standard reduces the protocol overhead to enable operation over constrained networks. We are simply not sure what impact this reduced functionality will have on security at this stage.

Turning to TCP transmission next, this is a very well-known transmission protocol. However, once again it is not suitable for use with often dormant IoT nodes where power consumption is typically minimised. UDP does not have any handshaking and is therefore typically being used. TCP does not work with dormant nodes or with excessive packet loss. Again, the trend has been to simplify an existing approach.

We next turn to the two security standards of most importance Transport Layer Security ("TLS") and Datagram Transport Layer Security. TLS requires TCP to function and will not work with UDP. UDP provides a level of security for constrained devices, but will it be enough in the future?

We therefore conclude that Ofcom has a pivotal role to play in ensuring the development of standardisation in general and security and resilience issues in particular. We previously suggested in our 700MHz response that Ofcom/BIS/DCIS might consider outsourcing standards tracking activities to neutral companies like ourselves to save money but still ensure that the UK was able to catapult its IoT vision beyond the UK rather than develop what turn out to be "dead end" solutions. The benefits of doing so far exceed the likely costs.

1.50 ***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.*

There is soon to be a new EU Data Protection Regulation, which is to be discussed in Council only days after this consultation closes. Based on what we know to date, the new EU regulation will place considerably higher duties data controllers, with significantly higher penalties for any breaches.

A key objective of the IoT and big data is the predictive analytic functionality is makes possible, and to what use that functionality is put. These uses could be for commercial gain, improved safety, enhanced security, trend analysis – or simply switching your toaster on.

The UK already has an Information Commissioner's Office ("ICO"), that has a full time focus on this domain, we would therefore suggest that it would be prudent for Ofcom to liaise regularly with ICO. The key issues, we believe, will emerge will surround trust. Consumers will resist allowing their data to be used if they are concerned about the ways in which it might be used.

One only has to recall the Phorm case in the UK where BT and Phorm in 2008 secretly intercepted and profiled of Internet traffic of thousands of customers without their knowledge or consent, to provide specifically targeted ads to them based on their browsing habits. We conclude that an appropriate balance needs to be struck that protects citizens rights and the needs of both companies and the State. The complex trade-offs involved are already being made and appropriate laws devised. Ofcom's role is more likely to be in assisting with downstream enforcement actions and ensuring compliance of the operations of electronic communications networks and services with all applicable UK and EU statutes. We do though have concerns that Ofocm will be under resourced in this domain and may be unable to cope in an era of continued budget cuts.

1.51 ***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.

There is no doubt at all in our minds that IPv6 will provide the address space needed in the quantities needed. The UK already has significant issues with the availability of IPv4, and so Ofcom may have to take leadership in mandating IPv6. Might this be possible by means of a condition that could be attached to all General or Individual Authorisations? However this would mean that all General Authorisations would then have also to be notified to Ofcom. We therefore recommend urgent dialogue with the EU Commission because we would want to ensure the cross border interworking of IPv6 (and the use of open standards, including DTLa and 6LowPAN referred to earlier).

Currently we have not even got things working in the UK. It is possible to buy end-to-end IPv6 compatible equipment in the home, but it is not possible to get an IPv6 service beyond a home hub and out onto the networks. This is an extremely serious issue which we tackled in more detail in our recent response to DCIS.

1.52 ***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.*

For mass sensor deployment, cost and power are critical functions. Battery technology has not advanced rapidly in recent years, the solution being rather to power down to save energy, not to make the cells themselves last longer. Longer lasting cells, if-and-when developed, will command a price premium because they will be using new and novel technologies. Solar certainly has some role to play – even in the UK. Memory remains power hungry (including flash memory), whilst Linux is not well suited to low power environments and is "memory and battery intensive" in use. Perhaps the way forward will mirror standards development elsewhere for the IoT and a new "Linux Lite" or some other stripped down O/S will evolve since it need not be overly complex. This seems likely.

UK(Ofcom?) led and funded research in this area would be beneficial.

1.53 ***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 the "digital native" generation comes of age, digital literacy will become less of an issue. What however will not go away are concerns about trust and security. Unless consumers clearly know what's in all this for them they may turn against what could just as easily be

seen as “big brother” technologies which could be highly intrusive and evasive. If consumer data is being monetised for commercial gain, then why should consumers themselves not share from the gain that their data brought about?

1.54 ***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.*

We touch on this through the response in several places. Predictive analytics is one of the key benefits of the IoT. This information can and will be used in a helpful, benign or sinister way.

It is actually essential that there are checks and balance in place to protect citizens and consumers – and also the State. Where such boundaries end up being drawn “post Snowden” is a matter for the legislators and the Courts.

1.55 ***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.*

It is essential that *International* development focuses on IPv6 and open industry-driven standards. Ofcom’s role should be to capture and share information on the standards evolution in order to fulfil its statutory duties and to help promote the UK’s position in standard setting. Its role should not though extend to standards development. ETSI could prove particularly important for the development of the EU market where the UK already has strong commercial relationships and can therefore most quickly monetise activities.

1.56 ***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.*

According to data we have seen from the Economist Intelligence Unit report “The IoT Business Index” from a survey conducted last year, “by region, European businesses are fractionally in front.”

We think that in order for Europe to stay there, and for the UK to be at the forefront, Ofcom’s key interventions (in no particular order) are likely to need to be in relation to:
1 Access to the spectrum

2 What is being transmitted (content)
3 Where and how data is being stored and secured
4 Promotion of open and interoperable standards
5 Prevention of abuses of a dominant position
6 Protection of privacy and security
7 Furthering the interests of citizens and consumers
8 Making the UK an attractive place to do business
9 Extending its standards monitoring activities (of particular help to SME's)

Of particular importance at this stage is the final point. The listed below are the key standards that drive today's Internet, and we think they will also be the foundation of tomorrow's IoT in varying forms. Their development, which we have already touched upon, will be absolutely critical – so if we want to stay in front we have to lead the charge.

They are

1. IPv6 (and IPv4) – LEAD in pushing for International deployment.

2. TCP/UDP – Transmission Control Protocol is the Internet's primary transport layer, but it is UDP evolution that is of critical importance at this stage. TRACK UDP.

3. HTTP – This is the Internet's application protocol. It's how every web page is constructed and it's the foundation of data exchange on the Web, but it is CoAp (Constrained Application Protocol) development that manages data exchange for constrained devices. TRACK CoAP

4. TLS – Transport Layer Security provides communication security over the Internet, but DTLS that works for constrained devices. TRACK UDP

We feel that Ofcom would hugely assist IoT development by reporting on these mission critical fields on a regular basis, so that SME's in particular would be able to focus their limited resources to best effect. We would be happy to explore further how this might be done if Ofcom does not have the resource to develop the idea.

END