Promoting investment and innovation in the Internet of Things

Ofcom Call for input published on 23 July 2014

BT response

1st October 2014

Executive Summary

BT welcomes Ofcom's work to date regarding the development of the Internet of Things (IoT) market and of its own role in enabling this market to develop most effectively. We agree that these developments could be transformative for consumers and businesses, and that there is likely to be an important role for Ofcom in facilitating this process.

For example, Ofcom has identified some key market sectors – Healthcare, Transport and Energy – in its call for input paper[1] that will form the early basis of new IoT applications enabled by new/existing devices and connectivity. Whilst many applications may emerge naturally from the market, they will be innovated by specific market sectors and countries. Ofcom should work with communications and cross-sectoral NRAs (e.g. Ofgem) to ensure cross border & sector mechanisms such as interoperability, number portability, availability of new wireless spectrum and roaming policies support innovation and take-up of IoT.

We therefore very much welcome Ofcom's consideration of these key issues.

Ofcom's paper lays out a number of policy issues such as: security and privacy; interoperable IoT standards; risk of cyber threats; access to big data; and the potential need for additional spectrum. These issues are not new for industry and Ofcom as they impact existing and varied communications and applications. Ofcom clearly has an on-going role in ensuring that these established policy areas evolve in a consistent manner to facilitate the IoT market from both a supply and demand-side perspective.

Additionally, Ofcom should recognise that the driver for efficient growth in the new IoT market will require a larger and diverse set of supply-side players in each market sector. Ofcom's role therefore goes beyond its role of regulating prices for access to infrastructure bottlenecks. One key activity will be to ensure that new market entrants are aware of and act in accordance with relevant regulation and legislation. Ofcom must also recognise that additional issues and challenges such as quality of service (QoS) demands, network resilience and potential incremental bandwidth requirements could arise and need to be considered especially in context of today's regulated access and backhaul networks. Communication networks have become a critical national infrastructure and Ofcom should seek to avoid their commoditisation which will not support national economic prosperity. Appropriate incentives will be required especially for suppliers of regulated assets to support future demands of what could become critical infrastructure.

Ofcom's commissioned study[2] noted the likely future demand of IoT applications on spectrum requirements. In BT's view, the IoT market segments will require a mix of wireless and fixed communications, and as Superfast Broadband (SFBB) take-up increases, one can envisage a wide range of applications being delivered in the home, workplace and on the move. Ofcom should ensure that outcome is managed appropriately from the various policy perspectives such as technology neutrality, common standards and switching of devices and users.

[1] Promoting investment and innovation in the Internet of Things, Ofcom, 23rd July 2014
[2] M2M Application Requirements and Their Implications for Spectrum, April 2014

Spectrum requirements and management

Spectrum has already been successfully deployed to provide IoT services, and there is consideration of operating IoT devices on a *shared/ licensed-exempt basis* in TV white spaces and/ or the 870 – 876 MHz band. Whilst this available spectrum has enabled early innovation, it may also be possible to use other similar bands which have been identified for "Short Range Devices". Ofcom should consider making these bands available to enable market innovation by existing and new entrants.

A key role for Ofcom should be to manage the availability and allocation of licence exempt spectrum to ensure that fair and equitable use is achieved by all market players.

Where a more reliable environment is required, for health or e-payments applications, deploying spectrum on a *licensed basis* could be preferred. Currently, the deployment of existing licensed networks (e.g. GSM) has been adapted to carry M2M data and fall into this category. To develop a competitive IoT market, BT would like to see specific frequency bands identified for such purposes. We acknowledge and support the principle that bands are normally assigned on a service neutral basis, and that regulations for use of a band can be optimised to suit a particular application. Ofcom should ensure fair access is provided to such licensed spectrum, especially if it were to become an enduring bottleneck.

Ofcom must strike the balance of sufficient spectrum that will enable multiple M2M/IoT licences to be awarded from the outset, or alternatively licence holders of critical or unique spectrum assets should be mandated to offer wholesale regulated access to all users that are based on standards.

Network related issues

Service level competition, rather than network infrastructure competition with wholesale access, is clearly good for consumers and the industry. We have witnessed the efficacy of this in the UK broadband sector. From an economic investment perspective, there will be cases, either due to limited asset availability such as spectrum and/or limited ARPU by application, where it may not be economically efficient to have more than one provider in a given geography for a particular service. IoT is a case in point where the bandwidth and performance requirements for a specific application could be low and therefore the revenue could be disproportionate to the total standalone infrastructure investment costs. Unlike traditional telephony or broadband (fixed or mobile), where the ARPU is designed to recover standalone costs, the IoT economic model will need to be developed such that devices utilise common infrastructure and/or appropriate incentives are made available to the communications infrastructure providers to invest, especially in hard to reach and low volume take-up geographies. This requirement is especially relevant for IoT applications that have yet to be launched and/or achieve mass market scale. Ofcom should monitor such specific market developments by application and geography and enable the appropriate regulatory mechanisms to incentivise investment and prevent market failure on the supply and demand side.

BT supports the principles of openness, adoption of standards and technology neutral networks as these are key enablers of innovation and competitive markets. The lack of readily available and efficient connectivity solutions would lead to vendors at the application level being locked out if there were a single operator that was not appropriately regulated by Ofcom to provide wholesale open network access from a price, interface, availability and service perspective. At present, M2M applications and devices are largely driven by industry specific sectors e.g. transport and health, on a global basis to reflect these industry structures. Adopting alignment of key principles is a fundamental requirement if the UK is to become a leader in the development of IoT services.

IoT applications could place increasing demands on existing constrained networks; homes and workplace environments could require greater network uptime and faster repair times. Such improvements in network performance can only be achieved if Ofcom recognises these performance requirements and makes the appropriate allowances for suppliers of regulated assets to support such future demands across fixed and wireless networks.

Security, Resilience and Data privacy

The global M2M market is forecast to achieve a quarter of a billion connections in 2014 according to GSMA[3], and as take-up increases across market sectors, global geographies and networks, the policies governing data security, privacy and network resilience become critical enablers for development and adoption.

Regulation and public policy exist today for data and internet security. BT believes that the UK should build on these security policies and legislation that have been established at the EU and global level by bodies such as ISO, ITU, OneM2M ETSI and the BSI.

These principles must be applied to IoT providers and ideally engineered-in at the design phase of devices and network provision, especially where no direct human or consumer intervention is required in setting up or operating the service.

In the early stages of market development, certain network access technologies and protocols could be proprietary, limiting the need for interoperability, for example in portability between networks. However, as IoT technologies, applications and networks mature and naturally converge, the principle that devices should be able to communicate *securely and resiliently* on any available network on a technology and network neutral basis should apply.

Personal data issues are not unique to M2M/IoT applications and will need to be addressed for this emerging market. These issues are well understood; whilst BT does not believe that any change to regulation is warranted at this stage, it is important that market developments are monitored to ensure that the principles can still be appropriately applied at all times.

In the case of commercially sensitive data, especially for providers of networks and services, BT sees the following exposures that should be mitigated: manufacturers device topology; Service Providers' network topology; Service Providers' coverage, network capacity and volumes by

[3] From concept to delivery: the M2M market today, GSMA, February 2014

application. Such exposures, if left unaddressed, could enable cyber attacks or inadvertent loss of personal data.

Ofcom should monitor market developments and ensure that all supply side stakeholders are aware of and adhere to their specific role and responsibilities such as educating end users where appropriate and gaining their consent for access to and sharing of information. As noted above, where additional requirements are placed on bottleneck infrastructure providers to support critical applications such as real time transport routing or health applications, providers must be able to recover their investment.

In summary, the M2M/ IoT market is rapidly developing on a global basis, deploying a mix of different technologies to support fully mobile, fixed and hybrid devices and cross-market sector applications. Each market application will have a distinct set of commercial, technical and geographic requirements that will require a balance between industry led innovation and practice, balanced by a proportionate regulatory intervention approach to support successful market development and consumer benefits on a pan-European and ultimately global basis. No new regulatory interventions are indicated at this early stage; however Ofcom has a valuable role in monitoring developments in alignment with other relevant regulatory bodies to ensure powers and their application remain appropriate.

1.0 Responses to Ofcom's specific questions

Section 1.47: Spectrum Requirements

As stated above, the role of fixed communications in enabling IoT applications and making these available on a mass market basis is fundamental. Ofcom must also consider fixed network requirements alongside wireless/ spectrum issues to ensure the right investment and market entry conditions are created and maintained for the broadest range of IoT services.

The category of IoT communications covers a broad range of applications with widely differing requirements. While there are expected to be many sensors producing small amounts of non-time critical data and which do not require significant levels of security, other applications will be "mission critical", or carrying information that needs to be transmitted in a secure fashion which would have very different spectrum requirements.

A common factor in many IoT applications is that remote sensors will typically be limited in levels of power of the transmitted signal; the application or operating environment may necessitate a battery lifetime of months or even years without replacement. They may also need to operate over significant ranges (possibly of the order of kilometres). As a consequence of these and other factors, efficiency and good signal propagation will be essential in many cases and therefore IoT communications are expected to be predominantly in the frequency bands below 1 GHz.

Licence exempt operation, band sharing

There is consideration of operating IoT devices on a shared basis, typically under a licence exemption (e.g. in TV white spaces and also the 870 – 873 MHz band). We believe that these will be a good start for many applications, particularly as this spectrum is already available.

For applications for which power consumption is not so critical, the 2.4 GHz band could be deployed, although the proliferation of other devices using this band is expected to make the band only suitable for short range IoT operation (e.g. ZigBee networks within a home or office).

At some stage utilisation will reach the point where further use leads to performance degradation. BT believes Ofcom has a role in considering what mechanisms should be adopted to reach a balance between the flexibility resulting from licence exempt operation and fair and equitable use of such spectrum resources. We also believe that early consultation on the options and approach to be adopted in the short term could assure all market players that long term developments were viable, and justify investment in the UK market. The recently announced exercise regarding authorisation of high duty cycle Network Relay Points in the 870-873MHz band is an example of such a consultation.

Licensed operation

There will be some cases for which a more reliable environment is required, and these should consider operating on a licensed basis. At present the only examples of this are the deployment of existing licensed networks (e.g. GSM) being adapted to carry M2M data. We believe that in the future specific bands should and will be identified for IoT purposes. (We acknowledge that bands

are normally assigned on a service neutral basis, and we support that principle, but the regulations for use of a band can be designed to suit a particular application, to encourage users to use the band for that purpose.) Ofcom should ensure fair access is provided to such licensed spectrum, especially if it becomes an enduring bottleneck.

There are discussions about identifying paired spectrum in the 700 MHz band for IoT, which is expected to be assigned on a licensed basis, although it is recognised that the 700 MHz band is unlikely to be available for IoT for several years.

In anticipation that a band is identified for IoT purposes on a licensed basis, some important questions arise regarding the award of licences for the band. There is a risk that a monopoly (or very limited competition) could be established that would limit rollout, market choice and innovation.

Either there needs to be sufficient spectrum identified to enable multiple IoT licences to be awarded from the outset, or alternatively the IoT licence holders should be mandated to offer wholesale regulated access to all users. Given the nascent nature of IoT, with potential for enormous growth, we believe that regulated wholesale access should be mandated to allow small "virtual" IoT networks to grow taking advantage of the infrastructure created by the licence holders.

Section 1.48: Network-related issues

The scope of IoT Services arguably includes the end application(s) which could run on existing IT assets as well as the collection of data from devices. We agree that this could be over a number of technologies but there are more options (listed below) and to ensure the full range of service and enabling technologies and services are considered should be all included in Ofcom's future considerations:

- Wi-fi
- RFID
- NFC
- Cellular
- Fixed ADSL or fibre-delivered broadband services
- Novel Low Power radio solutions
- Mesh radio e.g. Mobile WiFi
- Solutions for mobile devices e.g. tracking unpowered moving items

BT believes that a single network infrastructure investment approach that enables service level competition by spectrum sharing or wholesale access is most efficient. Indeed, for many IoT applications where the bandwidth and performance requirements are low and therefore the revenue would be equally limited, investment in dedicated infrastructure would be uneconomic. Example applications might be smart waste bins. Loading costs into this market could be counterproductive at least initially – this could lead to a franchise model by geography or location for some services. Ofcom needs to monitor specific market development by geography and ensure the appropriate regulatory mechanisms are put in place to prevent market failure.

Appropriate incentive mechanisms will need to be established to manage the risk of building these networks ahead of demonstrable demand. There is a vicious circle that manufacturers may not build chipsets/devices until they see access network investments; conversely access providers are not willing to invest if there is nothing to connect. The risk is that we revert to closed, vertically integrated solutions that are ultimately less efficient and result in sub-optimal prices to consumers.

Delivering IoT services within home or office environments provides the opportunity to utilise a broadband connected gateway device to provide local wireless connectivity to devices (e.g. via a Home Area Network). There are likely to be coverage and cost benefits for this type of approach that could also enable the support of multiple wireless technologies (e.g. ZigBee, Z-wave, 6LoWPAN etc.) to support connectivity of a wide ecosystem of IoT devices within a building environment.

Section 1.49: Security and resilience

BT believes that maximum benefit from the development and adoption of IoT technologies can only gained if there is general recognition and acceptance that security and resilience of services is assured on a long term basis.

A wide range of factors need to be considered in this context and in setting out suitable responses, stronger definitions relating to security and resilience aspects of M2M and IoT services may be required.

IoT services are likely to have a number of characteristics that, whilst building on existing and proven approaches, will require additional consideration:

- The volume of devices in use – potentially into the billions;
- Applications will have a wide range of minimum security requirements
- The devices will need to operate autonomously for long periods of time
- Operation via battery power indicates that efficiency in energy use will be a priority, restricting the data processing resources available for security functions.
- Many devices will be installed in public spaces where physical security will be minimal.
- The volume of devices employed and a range of other factors could imply even very low levels of device failure results in disruption to wider services

As a consequence of these:

- BT believes that it is important for the UK to support and build on the security work already completed in bodies that have EU and global recognition in ISO, ITU, OneM2M ETSI and BSI (amongst others).
- That whilst existing public policy, legislation and regulation is appropriate, this needs to be kept under review as the market develops. Specific attention may be indicated where use (or misuse) of such services crosses traditional regulatory boundaries.
- That potential conflict between existing regulatory requirements and beneficial IoT developments should be addressed in advance. (As one example, applications requiring high levels of security may conceal the identity or specific location of devices, or have end to

end application encryption applied independently to that of the service provider. Whilst avoiding the costs and complexity associated with providing high levels of security in the service provider domain where not all applications require it, this could conflict with requirements placed on communications service providers with regard to lawful interception).

- In the early stage of market development, proprietary network access technologies and protocols require limited interoperability, for example in portability between networks. However, as IoT technologies and applications mature and converge, the principle that devices should be able to communicate on any available network on a technology and network neutral basis should apply.
- That within any standards applying to devices deployed in IoT-type services, consideration is given to the means of containing the effect of faulty devices. (Whilst removing a device's validity in a service database restricts service to authorised devices, it would not prevent a physically faulty device from disrupting other services. Equally, any requirement to disable radio or other interfaces must consider the potential effect that inadvertent or malicious activation could have on certain critical applications).
- BT agrees with the statement that "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" but care needs to be taken that the requirements for these high end applications do not dominate security design, implementation and management at least at the outset. Otherwise it may not be possible to support all use cases at an acceptable cost.

Section 1.50: Data Privacy

For personal sensitive data BT sees that existing data privacy situations will need to be considered in the new M2M/IoT context. At high level, BT believes that approaches should be informed by;

- Ensuring that the area of consent to utilise data gathered by IoT services continues to follow accepted practices and principles in use today, adapted as required to remain relevant to the services being offered.
- That specific activity be initiated to ensure that citizens and organisations are fully aware of the benefits of these technologies and the controls and regulations in place to protect their interests and personal data (see Section 1.53: Digital Literacy).

Gaining informed consent

BT agrees that it may not be obvious to users that their data is being captured, especially if IoT devices and user interfaces are unfamiliar. However, approaches to the ownership of the various data sets should be proportional – in many cases IoT data will not allow individuals or their actions to be identified even without additional need for anonymization. New or additional regulation or legislation should only be considered where existing measures are clearly unable to provide the necessary protection. Information campaigns intended to promote awareness of IoT could usefully address any potential data privacy concerns and the proven means in place to address these. Existing approaches, such as "privacy by design" and the requirement for regular purging of data are tangible examples of existing best practice.

Section 1.51: Numbering and addressing

The use of mobile numbers to support certain wireless/M2M interconnections does to a large extent make sense, but does raise a question as to the potential impact that using fixed numbers to support wired interconnection would have on the current 01 and 02 ranges, especially in areas where number exhaustion is close to being a reality and would require short term action. Whilst the consideration of wireless interconnection does not mention the impact of ITU T E.212 resources (International Mobile Station Identifiers), the need to allow other implementations of interconnection, and the impact that alternatives may have on the availability of national telephone numbering resources, requires further consideration by Ofcom. One alternative to the use of current numbering resources could be the allocation of a new sufficiently neutral range with significant available resources (for example 05). Whilst not without challenges to support different technologies, it removes the impact that demand could place on existing numbering ranges.

The availability of IPv4 addresses is well known. The multi-stakeholder approach through the relevant Regional Internet Registries has sustained availability of these addresses. This approach should continue in the future. The deployment of IPv6, for this or indeed any other use, will reflect the need for such deployment, and respond to commercial drivers and operations.

Section 1.52: Devices

A key dependency for the development of a wide ranging and competitive market for devices in the UK and global markets will be the level of economic certainty and therefore risk facing device manufacturers to invest in these new markets. This will require both the creation and adoption of a range of standards (including for example radio and spectrum aspects and communication protocols for information representation). Some of these are yet to emerge. BT believes the activities of various standards development forums are key to delivering workable and acceptable standards required to underpin a successful UK (and global) standard.

UK-specific standards or requirements must be avoided where possible. Geographically restricted approaches limit the economic scope and incentives for potential suppliers which could result in a reduction in the rate of innovation, increased costs, and in extreme cases, marginalisation of the UK market. If the strategic objectives for adoption of IoT-based services in the UK include both manifesting the benefits of such services (particularly those which are inherently cross-border, such as logistics, energy etc) and building services and capacity to serve non-UK markets, such limiting factors should be avoided where at all possible.

Long-term stability of standards (supported by government policy and/ or regulation) will enable and promote efficient IoT development and consumer take-up. In industries where long asset lives are common such as energy, telecommunications and transport infrastructure, business cases can rely on low rates of replacement. In others, device refresh cycles can be significantly shorter but reducing the need for this can have implied benefits (for example in reducing the volume of obsolete electronic devices within the UK waste stream).

Section 1.53: Digital Literacy

Building UK capacity in both the skills to develop, deliver and operate IoT-based services, and an awareness and willingness by consumers to engage with such services are as critical as the underlying technology and regulatory frameworks in manifesting the broad-based benefits of IoT.

Citizen Engagement

Overall, BT believes it is important to build consumer confidence in the use of personal information if companies in the Information Economy are to continue to innovate whilst also protecting fundamental rights to privacy. BT is an active participant of the Information Economy Council http://www.techuk.org/about/information-economy-council which has identified the need for a consumer-focused voluntary framework of principles. The IEC is developing a prototype framework that builds on existing principles, such as those developed by the OECD but adds recommendations for: consumer comprehensibility, ethical product design, and trusted compliance processes that operate along the supply chain. The IEC believes that to build consumer trust, the principles must be simple enough for users to understand and be backed by independent verification of compliance.

Engagement programmes in other mass technology delivery programmes have the potential to provide useful insight and guidance for activity that may be required to build acceptance and engagement with mass-scale IoT deployments in the UK:

- The engagement programme of the Digital TV Switchover is generally regarded as being successful. Whilst data privacy and sensing/control of domestic environments were not necessary features of this, explaining the need for change and the benefits for citizens from what was a complex technical programme was critical.

- The initial programmes to introduce Smart Metering for electricity and gas in some geographies provides strong evidence that “compulsion” based approaches (for example highlighting increased costs, or fines, for citizens not installing new meters) can lead to a range of negative responses, hindering rollout or adoption of new services

- Whilst still in the very early stages, the Consumer Engagement Plan for GB Smart Metering, has sought wide input to inform its approach in a range of aspects, including data privacy and protection and potential concerns for health are receiving strong consideration.

Certain early IoT services in very specific vertical applications (such as street lighting, waste stream management etc.) are not dissimilar to existing services which have not led to significant concern. However, future developments which sense, transmit and analyse data derived on a more personal level would be more likely to give rise to legitimate questions and concerns. Responses relating to the detail of technical, security and data protection/privacy aspects are provided elsewhere in this submission. BT believes that gaining maximum benefit from such technological progress relies on at least acceptance, if not active engagement, from citizens.

Skills and Capacity Building

Skills that can support converging markets and technologies are increasingly important. Our experience tells us that developing and skilling a technical workforce to evolve with the converging markets such as mobility, TV, and IoT, amongst others, will create more opportunity for new products and new markets. Convergence is starting to dictate the skillsets now required from a new type of skilled workforce, which understand the fundamentals of convergence and potential resultant products and services. Deploying common infrastructure such as Superfast Broadband and developing this to support specific applications will ensure efficient deployment of skills, processes and systems that are replicable across all UK geographies.

Section 1.54: Data Analysis & Exploitation

The means to securely access, analyse and deploy data sourced from IoT services within an agreed framework is key to the economic and market drivers underpinning deployment. The insights and associated benefits for citizens arising from these are to be encouraged. In the early stages of market development, the source, ownership and value derived from IoT-sourced data is likely to be reasonably clear, in so much as the new communications technologies justify vertical and highly coupled applications that were previously uneconomic to deploy.

However, if this results in multiple, closed silos of information the wider potential of IoT deployments accruing from the analysis and resulting insight from multiple sources of data could be limited. Early investors and operators of services would be highly motivated to monetise the information collected by their service. Enhanced value from analysis of multiple datasets would probably represent a second stage of market development.

It is possible that new protections, regulation or legislation could be required in the future, although at this stage BT believes existing provisions are sufficient. This is a key area for Ofcom to monitor and ensure regulation and policy evolves to reflect both risks to consumers whilst balancing the potential benefits and innovation. The very limited number of situations generating new information or insights at an individual level and any controls required should be considered on a case by case basis as they occur.

End