Promoting investment and innovation in the Internet of Things

Call for input

Publication date: 23 July 2014

Closing Date for Responses: 1 October 2014

About this document

This document seeks stakeholders' views on the actions required to ensure that the UK takes a leading role in the emerging Internet of Things (IoT).

The IoT will lead to the introduction of many new and innovative services. It will allow data to be transmitted between many different types of devices, improving the safety of transportation, reducing the consumption of energy and improving our health.

Over the next few years, this is likely to be a major driver of investment and innovation in the communications sector, delivering significant benefits to citizens and consumers. In the longer term the IoT could change the way we live our lives.

There are some policy areas over which we have a clear role as an enabler of the IoT, including in managing radio spectrum, monitoring the security and resilience of networks and managing the use of telephone numbers. We welcome the views of stakeholders on how we should proceed in these policy areas. More broadly, we would also welcome views on whether there are other areas in which we could adopt a more proactive role.

Introduction

1.1 The Internet of Things (IoT) is set to enable large numbers of previously unconnected devices to communicate and share data with one another. This new connectivity has the potential to deliver significant benefits to citizens and consumers across a range of sectors, including:

1.1.1 **Healthcare:** Devices that monitor fitness and activity levels can help to prevent illness and encourage a healthy lifestyle. For the unwell, the IoT could enable a patient's condition to be monitored and managed remotely, allowing them to recover at home, rather than in hospital. This has the potential to both reduce healthcare costs and improve the medical treatment and care of patients;

1.1.2 **Transport:** Connecting vehicles to the internet could enable them to be tracked and have the performance of their engine and other mechanical components remotely monitored. Connected vehicles should be better able to avoid accidents by detecting and monitoring the presence of other road users; and

1.1.3 **Energy:** Connecting a wider range of household, office and industrial equipment to the IoT could enable their use of energy to be monitored and potentially changed, for example to switch to a power-saving mode or to use electricity on a cheaper tariff during an off-peak period. In these cases, the IoT has the potential to both reduce costs for consumers and the energy suppliers, and reduce environmental impacts through better management of scarce natural resources.

1.2 A significant amount of work by academia and industry to date has led to the development of a number of new and innovative IoT applications, standards and networks. The aim of this Call for Input is to allow us to develop a better understanding of these developments and of the role that we need to play to ensure that the UK takes a leading role in the emergence of the IoT.

1.3 In particular, we would like to form a more detailed view on the following points:

1.3.1 It is clear that radio spectrum will play an important role in enabling the IoT, given the need to support a potentially significant number of wireless connections. We are seeking input on the scale and nature of demand for spectrum, including how much additional spectrum may be required to support the IoT, if any; which frequency bands may be suitable; and whether an approach based on licensed or licence exempt access to spectrum is more appropriate;

1.3.2 Aside from spectrum, we recognise that the IoT has the potential to raise a number of other policy issues in which we have a role. Some IoT applications will require highly robust and reliable networks and we are therefore interested in understanding more about issues relating to network resilience and security. A specific and important aspect of network security is privacy of personal or commercially sensitive data; there will likely be a number of privacy issues and the IoT will only flourish if these are addressed;

1.3.3 IoT devices will need to be assigned one or more addresses in order to communicate with other devices. A number of address types could be

used, including telephone numbers or Internet Protocol (IP) addresses. The type of address may depend on the network to which the device is connected and whether the device requires access to the global internet, or a local, private network; and

1.3.4 Finally, and more broadly, we are interested in stakeholders' views on the nature of Ofcom's role. Generally, our view is that industry is best placed to drive the development, standardisation and commercialisation of new technology. However, given the potential for significant benefits from the development of the IoT across a range of industry sectors, we are interested in views on whether we should be more proactive; for example, in identifying and making available key frequency bands, or in helping to drive technical standards.

Defining the IoT

1.4 The IoT is a loosely defined term and is often associated with machine to machine, or M2M, communications. The two terms are related, but are slightly different:

1.4.1 M2M describes the interconnection, usually through the use of wireless technologies, of devices that previously would not have had the ability to communicate. Examples of M2M applications include the ability to track the location of a car or monitor the performance of its engine and mechanical parts.

1.4.2 The IoT is a broader term, describing the interconnection of multiple M2M applications, often enabling the exchange of data across multiple industry sectors. An example is the ability to manage traffic flow, reduce pollution and improve health by combining data from a range of transport, healthcare and environmental sensors.

1.5 For simplicity, throughout this document we will use the term "IoT" to refer to both the Internet of Things and its constituent M2M connections.

IoT connectivity between devices may raise new policy issues

1.6 In April we published the results of an Ofcom commissioned study[1] on the future demand for IoT applications and their likely spectrum requirements. In common with many other projections, the study predicted a significant growth in the number of interconnected devices in the future (almost 370 million in the UK by 2022). However, it also recognised that accurate growth estimates are difficult to make at this stage, given the relative immaturity of the IoT market.

1.7 Wireless technology is likely to be the preferred approach for providing many of the interconnections between IoT devices because it can conveniently support the connections between portable and mobile devices.

1.8 This interconnectivity between devices has the potential to raise a new set of policy issues, including:

[1] M2M Application Requirements and Their Implications for Spectrum, April 2014, http://stakeholders.ofcom.org.uk/market-data-research/other/technology-research/2014/M2MSpectrum

1.8.1 The need for additional spectrum and network infrastructure to provide wireless connections between devices;

1.8.2 The need for interoperable IoT standards to allow devices from different sectors to communicate with one another;

1.8.3 The security and privacy of the data gathered, stored and processed by IoT devices;

1.8.4 The need for citizens and consumers to be sufficiently digitally literate to understand both the potential benefits and risks of the data created by their devices being shared;

1.8.5 The vulnerability of devices to cyber threats and malware;

1.8.6 The ability of IoT applications to be able to access and utilise so-called "big data" generated and shared by other IoT applications and devices; and

1.8.7 The need for electronic addresses, including internet addresses and telephone numbers, to identify IoT devices.

1.9 In relation to these policy issues, we have a number of relevant duties and responsibilities, including under the Communications Act 2003 and Wireless Telegraphy Act 2006:

1.9.1 We have a general responsibility to encourage investment and innovation in relevant markets;

1.9.2 We are responsible for the efficient management of radio spectrum. This includes assessing future demands for spectrum and the mechanisms by which spectrum could be made available;

1.9.3 We manage the UK's telephone numbers, are responsible for ensuring that sufficient numbers are available to meet demand and for setting the policy on how numbers may be used;

1.9.4 We have a duty to regularly report to government on the state of the UK's communications infrastructure, including advising on the allocation of Internet Protocol (IP) addresses; and

1.9.5 We have duties under Article 13a of the European Framework Directive to ensure that measures are taken to prevent and minimise the impact of security incidents.

1.10 We are interested in better understanding how the wider set of policy issues listed above will be applicable to the IoT. This will help inform what facilitating role we might play, if any, in these areas to ensure citizens and consumers can benefit from future developments in the IoT sector.

Different types of IoT applications are likely to have different spectrum requirements

1.11 We have a duty to ensure the optimal use of radio spectrum, the scarce resource that underpins the wireless and mobile services on which many citizens, consumers and

businesses depend. This includes exploring new sources of spectrum demand and how to best meet this demand to deliver benefits to citizens and consumers.

1.12 The IoT was identified as a priority area in our recently published Spectrum Management Strategy[2]. In addition, our recent statement on spectrum sharing for mobile and wireless data services[3] noted the views of many stakeholders that making additional spectrum available on a shared basis might benefit the development of the IoT.

1.13 Different spectrum and network solutions are likely to be needed to meet the different operational requirements of the range of IoT applications. These operational requirements include:

1.13.1 **Range:** Does the application require the long-range transmission of data, or do devices operate in clusters, concentrated in a small area?

1.13.2 **Sensitivity to quality of service:** How sensitive is the application to reductions in connection performance caused by, for example, multiple devices contending for access to the same shared network?

1.13.3 **Connection speed and duty cycle:** Does the application only require the transmission of a small amount of data on an infrequent basis or higher speed continuous connectivity such as that required for video transmissions?

1.13.4 **Device costs and battery life:** Does the application involve the use of low cost commodity devices which require relatively simple wireless solutions? Do the devices require a long battery life due to the difficulties and costs associated with replacing them?

1.13.5 **Degree of network or technology openness:** Does the application require access to the open internet, or could it be supported within a closed, private network? Does the application rely on the use of open, interoperable technologies or data standards, or can it operate using a non-interoperable, proprietary approach?

1.13.6 **Network and data security:** How sensitive is the application to the loss of data through the accidental or malicious disabling of network equipment? Is the data captured, transmitted and processed by the application of a personal or commercially sensitive nature?

1.14 As illustrated in Figure 1 below, there are two broad approaches that might be used to meet the future needs of different types of IoT applications:

1.14.1 **Shared spectrum:** Here a range of different devices and device types share access to the same frequency band using industry agreed access protocols. This approach is well suited to low power, shorter range IoT applications, such as those requiring only local clustered connectivity around an individual, car, home or office. This approach can also reduce barriers to spectrum access and help enable wider cross sector innovation in IoT services;

[2] Spectrum Management Strategy, statement published on the 30 April 2014, http://stakeholders.ofcom.org.uk/consultations/spectrum-management-strategy/statement/

[3] The Future Role of Spectrum Sharing for Mobile and Wireless Data Services, statement published on the 30 April 2014, http://stakeholders.ofcom.org.uk/consultations/spectrum-sharing/statement/

1.14.2 **Dedicated spectrum:** In this case there are controls on which devices and device types can access and use the spectrum. This approach is well suited to wider area IoT applications where a good quality of service is required, such as those used to manage and control national infrastructure.

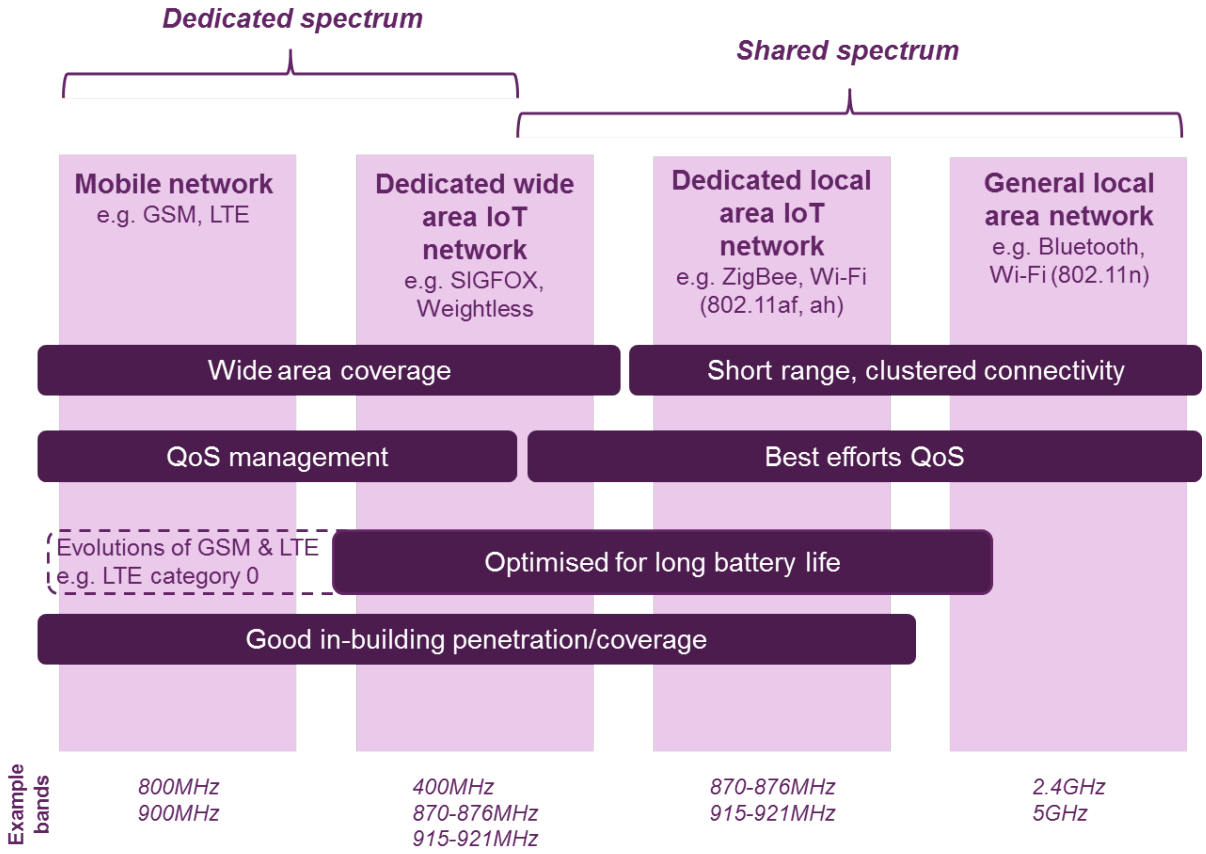

Figure 1: Proposed framework for considering spectrum requirements for the IoT

1.15 Due to their complementary nature it is likely that there will be a need to ensure a sufficient future supply of both shared and dedicated spectrum for use by IoT services. In reality, shared spectrum is normally made available on a licence exempt basis, whereas dedicated spectrum is typically licensed. In addition, hybrid approaches are possible, such as Licensed Shared Access (LSA), in which a licensee grants a licence to one or more other users to access spectrum on a shared basis.

Shared spectrum

1.16 The 2.4 and 5GHz bands that are widely used on a licence exempt (LE) basis by Wi-Fi devices are likely to play an important role in meeting some of the future spectrum demand for shorter range IoT applications.

1.17 There is also likely to be a role for additional, lower frequency spectrum to provide more comprehensive indoor coverage, such as that needed for smart metering applications. We have already taken steps to make such spectrum available. For example, we are currently working with a number of stakeholders to trial licence

exempt access to TV white spaces and have recently made the 870 and 915MHz bands[4] available for a range of uses on a shared, licence exempt basis.

1.18 A number of technologies are evolving that can support IoT applications in shared spectrum, especially for use over short ranges. The ZigBee standard has been developed to support very low data rate connections and low power variants of Bluetooth and Wi-Fi are emerging which are likely to help meet many of the specific future operational requirements of IoT services. Technologies such as SIGFOX and Weightless are also emerging that support communication over longer ranges and could be used in either shared or dedicated spectrum.

Dedicated spectrum

1.19 The approaches described above involve IoT applications and devices sharing access to spectrum and networks with other types of services. The potential drawback of this approach is that sharing spectrum with other services may impact the quality of service that can be achieved. This may be a particular issue for mission critical IoT applications.

1.20 Alternatively, spectrum could be dedicated for access by a particular technology or application. This spectrum could be made available on a licensed or licence exempt basis and may be particularly suited to use by emerging IoT-optimised technologies, such as Weightless and SIGFOX.

1.21 Mobile networks, using dedicated, licensed spectrum, are likely to continue to play an important role in meeting the needs of many IoT services, especially those requiring wider area coverage and a good quality of service.

1.22 For example, many first generation IoT services are using 2G cellular technologies, taking advantage of the relatively extensive coverage levels of existing networks. In the future, variants of mobile technologies, including systems based on GSM and LTE, are being developed to more efficiently support IoT traffic. These systems may use the spectrum allocated to mobile networks, such as the proposal to use 2×3MHz as part of the duplex gap and guard band in the future allocation for mobile broadband at 700MHz.

Gathering views on spectrum issues

1.23 From the perspective of future spectrum availability, we have recently published our Mobile Data Strategy[5] which identifies a range of potential future bands for mobile use. In addition, preparations are currently being made for the ITU-R World Radiocommunications Conference 2015 (WRC15). Agenda item 1.1 is specifically addressing the availability of spectrum for mobile broadband applications over the coming 10 to 15 years.

1.24 Estimates for future spectrum demand are based on a broad range of mobile services, including both conventional person-centric communications and the IoT. However, there may be a risk that some of the spectrum requirements for IoT

[4] The 870 – 876MHz and 915 – 921MHz bands were made available on a licence exempt basis on 27 June 2014. We will also be consulting on proposals to authorise the use of higher duty cycle Network Relay Points in the 870 – 876MHz band.
[5] Mobile Data Strategy, statement published 28 May 2014, http://stakeholders.ofcom.org.uk/consultations/mobile-data-strategy/statement/

applications will be different to the requirements for mobile communications more generally and may be overlooked.

1.25 We welcome stakeholders' views on whether the approaches described above are likely to be sufficient to meet the future spectrum demand for IoT services. We would also welcome views on the proposed framework shown in Figure 1 for considering the role different spectrum bands and allocation approaches might play in the future IoT landscape.

1.26 Where stakeholders believe that there is a need for additional spectrum, we welcome views in particular on:

1.26.1 **Frequency band:** Does the demand suggest a particular frequency band, or could a number of bands potentially be used? Would any new frequency bands need to be harmonised for IoT use internationally?

1.26.2 **Authorisation approach:** Should any new spectrum bands be licensed to one or more network operators, or would a licence exempt approach be more appropriate? Should a single, national approach be developed, or is there benefit in adopting multiple, location-specific approaches?

1.26.3 **Coexistence:** Could some IoT applications coexist with existing users of the spectrum, either in the same or adjacent bands? What steps could be taken to reduce the likelihood and extent of interference?

Network security and data privacy

1.27 In addition to our responsibilities for spectrum management, we have duties under Article 13a of the European Framework directive to ensure that measures are taken to prevent and minimise the impact of security incidents on users and ensure the continuity of access to services. In this case, security is defined as the confidentially, integrity and availability of a network or service and therefore these duties include a provision on the confidentiality of data, i.e. data privacy.

1.28 Our guidance on Article 13a states that the confidentiality of personal data is primarily the remit of the Information Commissioner's Office; however, Article 13a and sections 105A-D of the Communications Act furnish us with the power to pursue breaches of data privacy where deemed appropriate. We are beginning to consider how these duties could apply to the IoT.

1.29 Some IoT applications will require access to highly secure and resilient networks. This is particularly the case for applications that support or control aspects of critical national infrastructure, such as intelligent transportation or power generation. There will, therefore, be a need to develop approaches for protecting IoT networks, devices and applications from a range of threats, including component failure or cyber-attack. We are interested in understanding the scale and nature of security and resilience risks and views on the steps to be taken to mitigate these risks.

1.30 There will also be some issues related to the capture, exchange and processing of personal or commercially sensitive data. Some of these issues may be common to networks used for human-centric communication, such as the capture of personal information by smartphones. However, the development of the IoT will lead to new privacy issues; for example, it may not be obvious to users that their data is being captured, especially if IoT devices and user interfaces are unfamiliar.

1.31 There is a danger that these privacy issues could hinder the development and widespread take-up of the IoT if they are not addressed. We are therefore interested in stakeholders' views on the scale and nature of privacy issues that will emerge.

Numbering and addressing

1.32 IoT devices will need to be assigned addresses so that they can be identified on the network and communicate with other devices. There is a range of options for addresses, depending on the network technologies used and whether the devices or applications require connectivity to the whole internet, or a local, private network, specifically:

1.32.1 Where devices are connected to a conventional mobile network, a telephone number could be used. This mirrors the allocation of telephone numbers to mobile phones;

1.32.2 Where the IoT application requires access to the global internet, a public internet protocol (IP) address could be used; and

1.32.3 Where the IoT application only requires access to a closed network, a private IP address, or some other form of locally recognisable address, could be used.

Mobile telephone numbers

1.33 IoT devices connected to a mobile network could, in principle, use a conventional telephone number for an address. However, if a significant number of devices were addressed in this way, this could put pressure on the relatively limited supply of new mobile telephone numbers. Our initial assessment suggests that IoT devices are unlikely to use telephone numbers to the extent that this would put pressure on available numbers. We welcome views on this assessment, on the likely demand for telephone numbers for IoT devices and views on alternative addresses that could be used.

Global internet connectivity

1.34 There will be IoT applications that require access to the global internet, which will require devices to be assigned a public IP address. There are a relatively limited number of unique addresses conforming to the most commonly used format (known as IPv4[6]). If the IoT develops to include a significant number of devices, as expected, there may be pressure on the pool of available IP addresses.

1.35 To date, the scarcity of unique IPv4 addresses has been managed by the use of network address translation (NAT). This effectively increases the number of IPv4-addressed devices that can be connected to the internet by having additional network equipment act as a gateway between local networks and the global internet. However, the use of NAT could lead to more complex and inflexible network architectures and is unlikely to be a sustainable solution given the expected number of IoT devices.

[6] IP version 4 (IPv4) is the most extensively deployed version of the protocol used to identify devices on the internet. IP version 6 (IPv6) is a newer version of the protocol which, amongst other things, has a different address format to allow for a significantly greater number of connected devices.

1.36 This suggests that, where global connectivity is required, a move from IPv4 to IPv6 is necessary to open up a significantly greater number of unique addresses for IoT devices. We note that many communications providers are progressing plans to support IPv6 and that a more widespread deployment of IPv6-capable equipment could act as an enabler for the IoT.

Local connectivity

1.37 The use of the term "Internet of Things" implies that all devices and applications will be connected to the internet. In practice, there will be many IoT applications that will only require access to a closed, private network, with no wider connectivity. In this case a public IP address is not require and the entire range of IPv4 or IPv6 addresses can be used.

1.38 Alternatively, and depending on the size of the deployment, a different type of address could be used. For example, it would be possible to use hardware or medium access control (MAC) addresses to uniquely identify devices within a local area network.

1.39 We welcome views from stakeholders on all aspects of numbering and addressing, in particular on whether you agree with our initial assessments on demand for telephone numbers and IP addresses.

Ofcom's role in the development of the IoT

1.40 As outlined above, there are several aspects of the IoT that have relevance to our current activities, such as the management of spectrum and security and network resilience, and areas in which we have a supporting role, such as data privacy.

1.41 Generally, our view is that industry is best placed to drive the development, standardisation and commercialisation of new technology. However, given the potential for significant benefits from the development of the IoT across a range of industry sectors, we are interested in views on whether we should adopt a more proactive role.

1.42 We recognise that our role may differ depending on the specific aspect of the IoT being developed. For example, a more proactive role might be appropriate when new frequency bands are deemed necessary that might create new coexistence issues with existing services or where third-party access requires common interoperable standards between networks and devices. Conversely, we may need to be less involved in the development of standards for IoT-optimised variants of existing technologies.

1.43 In addition to views on how we might undertake our duties *differently* in order to support the development of the IoT, we are also interested in views on whether there is *anything new* we need to do. One example is in relation to so-called "big data". The IoT will involve the generation of a considerable amount of data from diverse sources. There are expected to be significant benefits from IoT service providers and third parties having access to this data, so that they can offer a range of innovative new services. We would be interested in stakeholders' views on potential barriers to the exploitation of "big data" to the benefit of citizens and consumers, and on whether Ofcom needs to take a role in removing these barriers.

1.44 More broadly, and in light of our general responsibility to encourage investment and innovation, we welcome stakeholders' views on the role we should take in driving the development of the IoT.

Call for input

1.45 As set out above, Ofcom is seeking to capture and better understand the full range of issues that might affect the successful development of the emerging IoT sector in the UK. Given this we are seeking views from all stakeholders on the themes listed below, plus any additional themes that respondents feel we should take into account. We would suggest that, where appropriate, reference is made to the framework shown in Figure 1 when responding.

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.).

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.

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.

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.

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.

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.

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.

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.

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?

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.

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.

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.

1.57 We are seeking views from stakeholders on all the areas set out above and any other issues you think we should consider.

Next steps and timescales

1.58 Over the coming months, we will continue to develop our thinking on the IoT based on stakeholders' submissions in response to this call for input and other internal analysis. Where possible, we will also engage with relevant industry groups involved in the development of the IoT.

1.59 Based on this inputs, we expect to develop a view on any next steps during the last quarter of 2014.

How to make submissions

1.60 Ofcom invites written views and comments on the issues raised in this document, to be made **by 5pm on 1 October 2014**.

1.61 Please send your response via:

1.61.1 The online web form https://stakeholders.ofcom.org.uk/consultations/iot/howtorespond/form ; or

1.61.2 By email - especially for larger submissions, including those with supporting charts, tables or other data – to iot@ofcom.org.uk attaching your response in Microsoft Word format, together with a consultation response coversheet (see next page).

1.62 Responses may alternatively be posted to the address below, marked with 'Call for input on Promoting Investment and innovation in the Internet of Things'.

Gary Clemo
Ofcom
Riverside House
2a Southwark Bridge Road
London
SE1 9HA

1.63 We do not need a hard copy in addition to an electronic version. Ofcom will acknowledge receipt of responses if they are submitted using the online web form but not otherwise.

1.64 Ofcom may publish responses to this CFI. Ofcom is subject to restrictions on the way we disclose and use information (see, for example, section 111 of the WT Act 2006). These seek to strike a balance between Ofcom's proper performance of our functions and protecting the confidentiality of stakeholders' information. They are relevant to material supplied in response to this call for input.

1.65 Ofcom will comply with our obligations and the restrictions in this regard. If your submission includes material which you consider is confidential, please indicate what that material is and why it is confidential. It is not helpful to make blanket claims of confidentiality for all submitted material. Please also provide a non-confidential version of your response (with confidential information omitted).

Cover sheet for response to an Ofcom consultation

BASIC DETAILS

Consultation title: Promoting investment and innovation in the Internet of Things

To (Ofcom contact): Gary Clemo

Name of respondent:

Representing (self or organisation/s):

Address (if not received by email):

CONFIDENTIALITY

Please tick below what part of your response you consider is confidential, giving your reasons why

Nothing ☐

Whole response ☐

Part of the response ☐

Name/contact details/job title ☐

Organisation ☐

If there is no separate annex, which parts?

If you want part of your response, your name or your organisation not to be published, can Ofcom still publish a reference to the contents of your response (including, for any confidential parts, a general summary that does not disclose the specific information or enable you to be identified)?

DECLARATION

I confirm that the correspondence supplied with this cover sheet is a formal consultation response that Ofcom can publish. However, in supplying this response, I understand that Ofcom may need to publish all responses, including those which are marked as confidential, in order to meet legal obligations. If I have sent my response by email, Ofcom can disregard any standard e-mail text about not disclosing email contents and attachments.

Ofcom seeks to publish responses on receipt. If your response is non-confidential (in whole or in part), and you would prefer us to publish your response only once the consultation has ended, please tick here. ☐

Name Signed (if hard copy)