Promoting investment and innovation in the Internet of Things

Summary of responses and next steps

Statement

Publication date: 27 January 2015

About this document

The Internet of Things (IoT) is set to enable large numbers of previously unconnected devices to communicate and share data with one another – its services span industries from agriculture and energy to transport, healthcare and much more, with the potential for significant benefits to citizens and consumers.

There are already over 40 million devices connected via the IoT in the UK alone. This is forecast to grow more than eight-fold by 2022, with hundreds of millions of devices carrying out more than a billion daily data transactions.

Ofcom has identified several priority areas to help support the growth of the IoT. Following feedback from stakeholders in 2014, these areas include spectrum availability, data privacy, network security and resilience, and network addresses.

We will explore how we can support and work with Government, the Information Commissioner's Office (ICO), other regulators and industry to facilitate progress on these issues at both a national and international level.

Contents

Section 1

Executive summary

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. Over the coming decade, the IoT is expected to grow to include hundreds of millions of devices in the UK alone.

1.2 This new connectivity has the potential to deliver significant benefits to citizens and consumers across a range of sectors, including:

1.2.1 **Healthcare:** Devices that monitor fitness and activity levels enable monitoring of existing conditions within the home, to treat illness and encourage a healthy lifestyle;

1.2.2 **Transport:** Collecting information from vehicles could help improve traffic flow, allow drivers to avoid traffic accidents and provide information for better vehicle design; and

1.2.3 **Energy:** Connecting a wider range of household, office and industrial equipment could enable their use of energy to be monitored and potentially changed, with implications for cost-saving.

1.3 Given these potential benefits we published a call for input in July 2014 which aimed to identify potential barriers to investment and innovation in the IoT sector. We also sought views on what role Ofcom might potentially play in helping overcome these barriers.

1.4 Based on responses to the call for input, in this document we set out our proposed next steps for supporting growth and innovation in the IoT. In summary these are:

1.4.1 **In terms of spectrum:** We have concluded that existing initiatives will help to meet much of the short to medium term spectrum demand for IoT services. These initiatives include making spectrum available in the 870/915MHz bands and liberalising licence conditions for existing mobile bands. We also note that some IoT devices could make use of the spectrum at 2.4 and 5GHz, which is used by a range of services and technologies including Wi-Fi. However, we recognise that, as the IoT sector develops, there may be a need for additional spectrum in the longer term. Given this we will continue to monitor IoT spectrum utilisation, in particular in licence exempt bands, to help identify when additional spectrum may be needed;

1.4.2 **In terms of network security and resilience:** We have concluded that as IoT services become an increasingly important part of our daily lives, there will be growing demands both in terms of the resilience of the networks used to transmit IoT data and the approaches used to securely store and process the data collected by IoT devices. Given this we intend to investigate how best to extend our existing activities on network security and resilience to include the relevant aspects of the IoT, working with the regulators of other sectors where appropriate;

1.4.3 **In terms of network addressing:** We have concluded that telephone numbers are unlikely to be required for most IoT services. Instead IoT services will likely either use bespoke addressing systems or the IPv6 standard. Given this we intend to continue to monitor the progress being made by internet service providers (ISPs) in migrating to IPv6 connectivity and the demand for telephone numbers to verify this conclusion; and

1.4.4 **In terms of data privacy:** In so far as the IoT involves the collection and use of information identifying individuals, it will be regulated by existing legislation such as the Data Protection Act 1998. We have concluded that a common framework that allows consumers easily and transparently to authorise the conditions under which data collected by their devices is used and shared by others will be critical to future development of the IoT sector. Given this, we will explore how we can support and work with the Information Commissioner's Office (ICO), Government, other regulators and industry to facilitate progress on this issue at both a national and international level.

The IoT has the potential to deliver significant benefits to citizens and consumers

1.5 The IoT describes the interconnection of everyday devices to provide a range of new and innovative services that will fundamentally change the way we live. This change will be driven by both the scale and variety of devices within the IoT.

1.6 There are currently in excess of 40 million devices in the IoT within the UK. A study[1] recently commissioned by Ofcom predicted that this figure will grow more than eightfold by 2022, when the IoT will consist of 360 million devices and more than a billion daily data transactions. The benefits of these connections will be delivered across multiple sectors and the range of devices whose role will potentially be transformed by the IoT include those in the transport, health and energy sectors.

1.7 Beyond these direct consumer benefits, additional benefits will be realised through the existence of a multiplier effect as a result of 'big data'. The volume and variety of raw data from such a diverse range of devices will likely stimulate innovation and new services across multiple sectors.

1.8 For example, an individual living at home with a long-term condition may benefit from the use of wearable sensors which monitor their health and trigger an alert if a problem arises. If the sensor detects that the individual's condition requires an ambulance service, this information may be combined with traffic data collected from roadside and in-vehicle sensors to inform the ambulance service of the quickest route to the individual.

The UK is already taking a leading role in the development of the IoT

1.9 A wide range of stakeholders recognise the potential of the IoT and are working to secure its rapid development. This is contributing to significant momentum behind the

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

development of new technologies that are optimised to support the specific requirements of the IoT, such as very low power consumption and efficient support for very low data rates.

1.10 In addition, UK-based companies are in the process of making significant investments in IoT networks. The initial focus of these investments is on the support of low bandwidth IoT applications, which can typically be accommodated within existing spectrum allocations. Examples include:

1.10.1 The trial of IoT applications as part of the ongoing whitespace pilot, such as the monitoring of river levels in Oxford;

1.10.2 The deployment of smart metering networks, which enable the remote reading of electricity and gas meters and can provide consumers with up-to-date and accurate information about their utility consumption; and

1.10.3 The ongoing rollout of a general purpose IoT network across a number of towns and cities that could be used to support a diverse range of applications.

1.11 The Government has also acknowledged the role that the development of the IoT can play as part of its broader growth and innovation agenda[2]. For example, in March 2014 the Prime Minister announced a significant increase in government funding for IoT projects, citing their potential to underpin a new "industrial revolution". In addition, the Government continues to fund the targeted development of IoT technologies and pilot studies through innovateUK[3].

The IoT raises a number of new potential policy issues

1.12 The IoT will not be a single network and will comprise of many different technologies and devices. Figure 1 provides a simplified generic overview of the IoT. This has four key elements:

1.12.1 **IoT devices:** As described above, the IoT is likely to grow to include hundreds of millions of devices over the coming 10 years, the majority of which will require wireless connectivity. The characteristics of these IoT devices will vary, depending on the applications they support;

1.12.2 **Wireless networks:** IoT devices transmit the data they have collected wirelessly to basestations, network access points or via advanced mesh networks, using a range of existing and emerging technologies. These wireless networks will require access to appropriate spectrum bands to meet different capacity and coverage requirements;

1.12.3 **Internet:** Connecting IoT devices to a wider network or the public internet means more devices can become interconnected and the data collected can be analysed and stored in the most appropriate place. However, this interconnectivity can also raise new network security and resilience issues; and

[2] In December 2014, the Government Office for Science published a review by the Chief Scientific Advisor, setting out views on steps the Government can take to achieve the economic potential of the IoT. https://www.gov.uk/government/publications/internet-of-things-blackett-review
[3] https://connect.innovateuk.org/web/internet-of-things

1.12.4 **Data storage and analysis:** Many of the future benefits from the IoT will be delivered by new services based on the analysis of data from a wide range of sources. Some of this data may be personal or commercially sensitive, so it will be important to ensure that it is stored and processed securely and with appropriate consent.

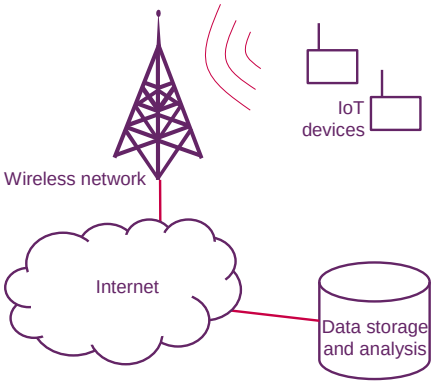


Figure 1: Key components of the IoT

1.13 The future operation of the IoT is likely to raise new policy considerations where Ofcom has a direct regulatory remit:

1.13.1 **Spectrum:** Ofcom is responsible for the efficient management of radio spectrum, including assessing future demands for spectrum and the mechanisms by which spectrum could be made available for a range of uses, including the IoT;

1.13.2 **Addressing:** Ofcom is responsible for the management of the UK's telephone numbers, including ensuring that sufficient numbers are available to meet demand and for setting the policy on how numbers may be used. We also have a duty to regularly report to government on the state of the UK's communications infrastructure, including advising on the levels of allocation and assignment of Internet Protocol (IP) addresses; and

1.13.3 **Network security and resilience:** Ofcom has a duty to ensure that appropriate measures are taken to prevent and minimise the impact of incidents that affect the security and resilience of networks and services.

1.14 The IoT also raises a wider set of policy issues, where Ofcom does not have a direct regulatory remit but where we might play a potentially facilitating role, in particular in relation to the secure collection, sharing and analysis of personal or commercially sensitive data.

1.15 Hence, addressing the full range of policy issues raised by the IoT is likely to require a collaborative approach, with regulators, Government, industry and other stakeholders working together to deliver outcomes that secure the full range of benefits.

Stakeholder responses identified four priority areas for enabling innovation and investment in the IoT

1.16 We asked stakeholders for their views on the potential barriers to innovation and investment in the IoT and the role Ofcom might play in helping address them. Based

on responses, we have identified the four priority themes shown in Figure 2 below. These themes have also been arranged to illustrate stakeholders' views on their relative importance.

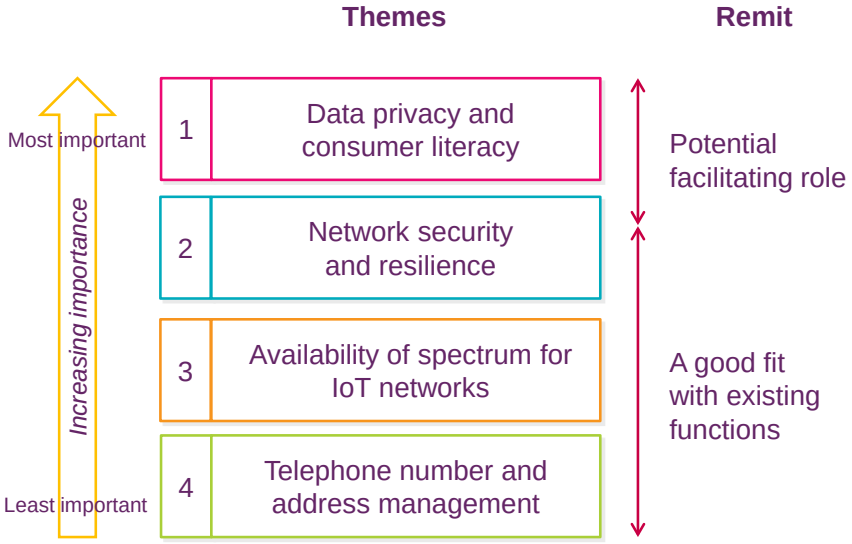


Figure 2: Summary of the priorities identified by stakeholders

Data privacy and consumer literacy

1.17 The most important theme identified by stakeholders was the need to adequately address consumer data privacy concerns. Whilst many stakeholder responses thought that the existing data protection regulations are likely to be appropriate for the IoT, they also identified a potential benefit in Ofcom working with others in a facilitating role, bringing together various stakeholders to define best practice for data privacy in the IoT.

1.18 Many responses also identified the need for industry-led approaches that will allow consumers to authorise easily and transparently the conditions under which the data collected by their devices can be shared. Respondents suggested that these approaches should ideally be agreed internationally, so as not to inhibit sale and use of IoT devices and services across international boundaries. We also believe that there will be scope for significant innovation on the part of industry in developing new ways to provide consumer protection.

1.19 In addition, some respondents identified the merit in advocating and communicating the potential benefits associated with the IoT more broadly. In particular, respondents mentioned raising consumer awareness on how new devices and apps will be collecting and using personal data to deliver benefits and services.

Network security and resilience

1.20 As the IoT develops and encompasses an increasing number of services on which citizens and consumers come to rely, it will become increasingly important to ensure that the networks delivering these services are robust and the data delivered over them is secure. This creates particular challenges as the traditional security approaches used in telecommunications may not be applicable in the high volume, low cost devices likely to be used by many IoT services. We acknowledge that

industry is aware of these challenges and work is ongoing to deliver secure and robust IoT networks and services.

1.21 Providers of networks and services are obliged under existing legislation to take appropriate measures to manage risks to security and resilience. The existing legislation does not explicitly refer to the IoT. However, to the extent that they fall under the definitions in the legislation, we believe IoT networks and services would be covered by these existing obligations.

Availability of spectrum for IoT networks

1.22 We do not currently consider spectrum availability to be a barrier to the development of the IoT in the short to medium term. The low data rates typical of the majority of emerging IoT applications mean that they can be supported within existing allocations. We have also taken steps to make additional spectrum available for IoT services, such as the 870/915MHz bands, and are examining the possibility of making spectrum between 55 and 68MHz available. We are also exploring options for liberalising the licence conditions for mobile spectrum to support the IoT. Many IoT applications that require short-range wireless connectivity could also use spectrum at 2.4 and 5GHz, which is used by a range of services and technologies including Wi-Fi.

1.23 However, the spectrum requirements for the IoT in the longer term are uncertain; the market is currently immature and future generations of IoT applications might have increased demands for spectrum (for example, if significant demand for high data rate video emerges). It will be important, therefore, to continue to monitor the development of the IoT to help anticipate and prepare for any significant changes in spectrum demand.

1.24 The international harmonisation of spectrum and standards is also likely to be vital for delivering economies of scale and lower cost consumer equipment; given the need for very low cost equipment for certain applications, this will be particularly important for the longer term success of the IoT.

Telephone number/address management

1.25 We believe that limits on the availability of telephone numbers will not be a barrier to the development of the IoT as a range of alternative identifiers, such as Internal Routing Codes, equipment identifiers and IP addresses could be used. We also consider that migration to IPv6 is likely to mitigate possible issues arising from the limited size of the IPv4 address space. This position is supported by our own monitoring of IPv6 migration, which was published in the recent Infrastructure Report[4].

Proposed next steps

1.26 Based on stakeholder responses and our own analysis, we set out below our proposed next steps in each of the four key themes. Some of these themes are a good fit with our existing functions, while for others there is the potential for us to play a facilitating role in seeking collaborative outcomes.

[4] Ofcom Infrastructure Report 2014, http://stakeholders.ofcom.org.uk/market-data-research/market-data/infrastructure/infrastructure-2014/

Data privacy and consumer literacy

1.27 We note that traditional approaches to data privacy may have some limitations in the context of the IoT. We therefore propose to work with relevant organisations, primarily the ICO, which has the duty for data privacy issues in the UK, to identify and explore solutions to data privacy issues in the IoT, in which Ofcom will play a facilitating role. We expect that this work will have both national and international dimensions.

1.28 On an international level, we propose to contribute to IoT-related work streams within relevant European agencies, such as BEREC. In the first instance, this will involve contributing to BEREC's ongoing activity on the implications of the IoT and machine-to-machine communications.

1.29 On a national level, we propose to undertake preliminary work, in collaboration with the ICO, Government and other stakeholders, specifically to understand the detailed nature of potential data privacy issues. On the basis of this work, we propose to identify key components of an approach or framework for data privacy for wider input from industry. This could include:

1.29.1 An assessment of the extent to which existing data protection regulations fully encompass the IoT;

1.29.2 A set of principles for the sharing of data within the IoT, such as ensuring that only the minimum amount of data for a given application is collected and limiting the time that data may be stored;

1.29.3 Exploring the need for work to better understand consumer attitudes to sharing data and approaches to providing consumers with the necessary information to enable them to make an informed decision on whether to share their data; and

1.29.4 In the longer term and as the IoT develops, exploring the merit of a consumer information campaign to highlight the potential benefits of the IoT.

Network security and resilience

1.30 We will undertake work to consider the impact of the IoT on our existing security and resilience guidance and whether this needs updating as a result. We believe that our existing overall approach of encouraging providers to consider security and resilience in line with established standards and best practice will be remain the correct one in the IoT domain. However, we may need to reference additional IoT-specific standards, or note the need for new ones where none currently exist.

1.31 As specific gaps in existing approaches are identified, we will coordinate with other stakeholders to develop standards and best practice relevant to the IoT. Existing national and international groups, which draw on industry and government experts, are expected to be the focus for any required technical work.

1.32 We note the comments we have received that this work is more likely to involve extending the scope of existing approaches, rather than creating entirely new standards and regulation. We will also be mindful of limitations of our powers in this area, which are focussed on securing networks and services.

1.33 We will continue to work closely with government colleagues on relevant issues, such as implementing the UK's Cyber Security Strategy and ensure relevant links to the IoT are made.

Availability of spectrum for IoT networks

1.34 We propose to continue our existing approach to identifying and making available spectrum for use by the IoT. This will involve:

1.34.1 Providing information to stakeholders about the bands that are currently available for IoT use;

1.34.2 Continuing to actively engage on IoT issues in public forums both nationally and internationally;

1.34.3 Tracking the developing size and nature of the IoT through existing information gathering processes, such as the Communications Market Report and the Infrastructure Report; and

1.34.4 Continuing our periodic monitoring of licence exempt spectrum use in a number of bands used by IoT devices. This will enable us to identify at an early stage whether congestion and interference is likely to occur.

Telephone number/address management

1.35 We propose to continue to monitor use of, and demand for, telephone numbers and network addresses by IoT devices. This will include monitoring of the deployment of support for IPv6 by internet service providers in the UK. We will continue to be mindful of the limited supply of mobile telephone numbers and support the use of alternative addresses and numbering where appropriate.

Section 2

Introduction

2.1 The Internet of Things (IoT) describes the interconnection of everyday devices to provide a range of new and innovative services. Over the coming decade, the IoT is expected to grow to include hundreds of millions of devices in the UK alone, bringing benefits to citizens and consumers across a number of sectors, including:

2.1.1 **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. This data could also be used for analysis to improve vehicle design over time. Connected vehicles should be better able to avoid accidents by detecting and monitoring the presence of other road users, and tracking information can also be used to improve traffic flow.

2.1.2 **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 both to reduce healthcare costs and to improve the medical treatment and care of patients.

2.1.3 **Energy:** Connecting a wider range of household, office and industrial equipment, such as lighting and heating, could enable their use of energy to be monitored and potentially changed, for example to switch to 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 resources.

2.1.4 **Asset tracking:** Incorporating sensors with wireless connectivity into objects can make it easier to track their location, and ensure that they are managed efficiently. Tracking solutions could apply to a wide range of different objects, including wheelchairs within hospital grounds or valuable industrial tools.

2.1.5 **Smart cities:** A range of technologies can be used to address some of the on-going challenges faced by cities and communities. For example, connecting public transport and infrastructure, including parking spaces, could make it easier to provide better information on congestion and transportation options; whilst connecting public rubbish bins could streamline refuse collection by ensuring that collection is optimised for when bins are full.

2.2 The IoT also has the potential to bring wider benefits to the UK as whole, by enabling growth and innovation in the economy. It is already stimulating the development of a range of innovative new technologies and devices; and UK-based companies are in the process of making significant investments in IoT networks.

2.3 The initial focus of these investments is on the support of low bandwidth IoT applications, which can typically be accommodated within existing spectrum allocations. Examples include:

2.3.1 The deployment of smart metering networks, with contracts across the UK secured in 2013;

2.3.2 The rollout of a wide area, general purpose IoT network. Sites have gone live in each of the ten target cities, allowing smart city and intelligent building applications to deliver potential benefits such as smart parking and waste level monitoring; and

2.3.3 Steps to develop technologies for existing and future mobile networks that support the efficient delivery of IoT services.

2.4 Government has recognised the potential importance of the IoT, not only in terms of supporting the UK growth and innovation agenda, but also the benefits the IoT may bring in terms of "big data". A key part of this is the multiplier effect, through which the volume and variety of raw data from a diverse range of devices will lead to a diversity of new services. The Government is interested in exploring how free and open access to public sector data could stimulate development by industry of a range of new and innovative services.

The IoT will be made up of a diverse range of applications and devices

2.5 There are currently in excess of 40 million devices in the IoT within the UK. A study[5] recently commissioned by Ofcom predicted that this figure will grow more than eightfold by 2022, when the IoT will consist of 360 million devices and more than a billion daily data transactions.

2.6 Alongside its potential size, one of the most striking characteristics of the IoT will be its diversity. The IoT will support a variety of new services, covering sectors including consumer electronics, healthcare, transport and manufacturing; many of these services will have quite specific characteristics according to the type of information they capture, where and how this information is processed and what is done with the results.

2.7 These characteristics will influence the capabilities of the devices and underlying networks that support the services. For example, some applications may involve the wireless transmission of data over long distances, while others may operate within a single room or building. Some applications may require access to highly secure and reliable networks, while for others a lower level of security may be sufficient.

2.8 This diversity of applications, networks and devices means that the IoT will heterogeneous in nature, comprised of multiple, different technologies and network architectures. Any steps taken to promote investment and innovation in the IoT will need to acknowledge and support this diversity.

[5] M2M Application Characteristics and their Implications for Spectrum, report for Ofcom, April 2014, http://stakeholders.ofcom.org.uk/market-data-research/other/technology-research/2014/M2MSpectrum

Intelligent buildings, utilities and cars will be major application areas

2.9 As illustrated in Figure 3, our study found that, at the end of 2013, the majority of existing IoT applications fitted within the category of intelligent buildings, followed by automotive, retail and manufacturing. Key applications include building security and climate control, vehicle tracking and electronic point of sale payment systems.

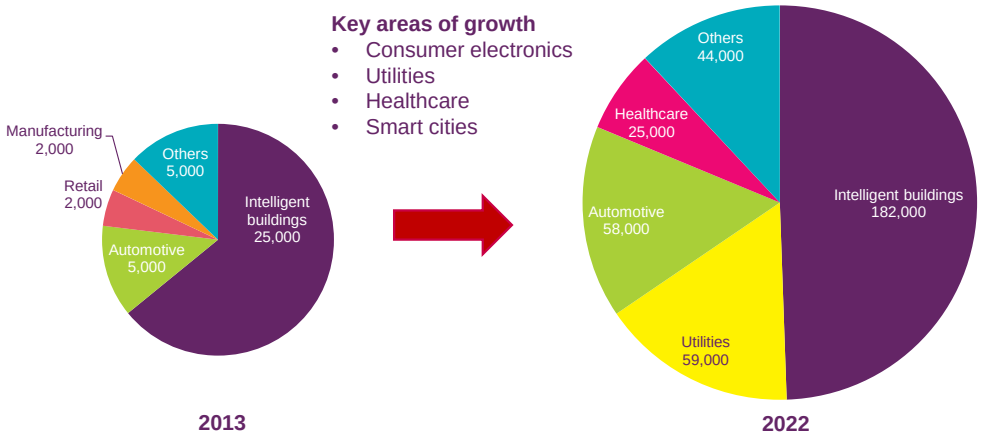


Figure 3: Potential number of IoT connections per application category in 2013 and 2022, in thousands

2.10 Intelligent building and automotive applications will also dominate the IoT market in 2022. However, the study also predicted significant growth over the coming 10 years for the categories of consumer electronics, utilities, healthcare and smart cities.

2.11 These figures illustrate the diverse nature of the applications that will be delivered by the IoT. It is clear that these applications with capture, share and process many different types of data from a range of sources. Many of these applications will be industrial in nature, involving the measurement or monitoring of systems, processes or the environment.

2.12 On the other hand, healthcare or consumer electronics applications could capture data that identifies individual users either explicitly, or implicitly when combined with other data. It will, therefore, be necessary to address any concerns about data privacy and trust if the IoT is to develop to its full potential.

Our call for input

2.13 There are some policy areas over which Ofcom has a clear role as the enabler of the IoT, including managing radio spectrum and the use of telephone numbers. More broadly, Ofcom has a general responsibility to encourage investment and innovation within our sectors, and a principal duty to further the interests of citizens and consumers in relation to communications matters.

2.14 In our call for input we sought views on how the IoT might affect the policy areas over which Ofcom has a clear role, plus other relevant areas in which Ofcom could play a supporting role. Based on responses to our call for input and our own internal analysis, we have considered the development of the IoT from a number of different perspectives.

2.15 The responses to the call for input highlighted four topics in particular, which we analyse in further detail below. In section 3 we summarise views on **data privacy and consumer literacy**, followed by **network security and resilience** in section 4. Section 5 covers views on the **availability of spectrum for IoT networks** and the final topic, on **telephone numbering and address management**, is covered in section 6. Section 7 summarises our conclusions and outlines our next steps.

Section 3

Data privacy and consumer literacy

3.1 Many of the future benefits from the IoT are likely to be delivered by new services based on the analysis of data from a wide range of sources. Some of this data may be personal or commercially sensitive, so it will be important to ensure that it is stored and processed securely and in the manner in which users have previously agreed.

3.2 If users do not trust that their data is being handled appropriately there is a risk that they might withhold its use, which could pose a barrier to the successful development of the IoT.

3.3 Many stakeholders noted that work was already underway to address data privacy challenges and that existing regulations, such as the Data Protection Act 1998, are likely to be appropriate for the IoT.

3.4 However, stakeholders identified the need for industry-led approaches that will allow consumers to easily and transparently authorise the conditions under which the data collected by their devices can be shared. We consider that these approaches should ideally be agreed internationally where possible, so as not to inhibit sale and use of IoT devices and services across international boundaries.

3.5 Given the relative immaturity of the IoT and the number and diversity of stakeholders, respondents highlighted a potential benefit in Ofcom working with others in a facilitating role to define best practice for data privacy in the IoT.

3.6 In addition, some respondents identified the benefit of advocating and communicating the potential benefits associated with the IoT more broadly. In particular, respondents noted the need to raise consumer awareness on how new devices and apps will be collecting and using personal data to deliver IoT services.

3.7 We discuss these points in more detail below.

The IoT will involve the capture and processing of a significant volume of data

3.8 While there are a number of different, precise definitions of the IoT, one common factor is the capture and analysis of data in order to deliver some wider benefit. Depending on the application, the data could be from a single type of IoT device or from a range of different device types. For example:

3.8.1 A sensor in a car monitors the engine's fuel efficiency and shares this data with the owner via a smartphone app;

3.8.2 A range of in-car sensors monitor the performance and state of the engine, transmission and suspension and shares this collated information with the owner via a smartphone app. In addition, the owner is able to share this information with friends and with the car manufacturer; or

3.8.3 Data from every vehicle's on-board sensors is collected and analysed with data on road, weather and environmental conditions in order to build a

detailed picture of traffic flow, to prevent accidents or to monitor trends in transportation.

3.9 The IoT is expected to generate, share and analyse a significant volume of data. One respondent noted that 90% of the world's data was created in the past year alone. A term often associated with both the large volume of IoT data and its processing is "big data".

3.10 Much of this data will be abstract in nature, yielding just the information captured by the IoT device. However, some devices may also capture data that is able to identify, either directly or indirectly, individual users; devices may also capture commercially sensitive data. It is reasonable to assume that such data should be kept securely and be subject to appropriate privacy guidelines.

3.11 In this respect, the IoT is little different in principle from conventional communications networks, that also have the ability to capture, store and process personal or commercially sensitive data. However, there are two factors that suggest that data privacy could raise additional issues for the IoT, namely:

3.11.1 The expected scale of the IoT could mean that personal data is collected by, and shared between, a large number of devices. For example, users' health and fitness data could be captured by a scales and a wrist-mounted exercise tracker; and their energy usage and physical presence could be inferred from their smart electricity meter, thermostat and lighting system; and

3.11.2 The IoT will be formed of a vast range of devices, many of which will not have the keyboards and screens that users are familiar with from their other communications devices. Users might, therefore, not know that their data is being collected, shared and processed and may find it harder to make an informed choice about whether to share their data.

3.12 There will also be an important international dimension to the IoT. Data captured in one country may be processed or stored in another and different countries may have different data privacy regimes. Addressing such differences will be particularly important if manufacturers market their IoT devices in multiple countries.

3.13 A number of stakeholders believed that, while the market is currently immature, future demand will be high for new and innovative services based on the capture and analysis of IoT data. One respondent described a staged approach, in which service providers first sought to monetise the data they collect before making it more widely available to other service providers. There was support for open data initiatives, such as the Government's plan to make non-personal, public-sector data available, and a recommendation that data should be low cost or free and in accessible and standardised formats.

3.14 There was broad agreement from respondents that concerns about data privacy could be a barrier to the development of the IoT. In particular, users concerned about privacy could choose to restrict, or completely opt out of, the sharing of their data. This would reduce both the volume and variety of the collected information, limiting the development of new services based on the analysis of "big data". In addition, respondents noted that there is a need to verify and provide reassurance that service providers use personal data in the way that has been previously agreed.

Industry is already taking steps to solve potential data privacy issues

3.15 Whilst many respondents acknowledged that data privacy could be a potential barrier to the development of the IoT, there was broad agreement that existing data protection regulations are appropriate and applicable. In addition, many respondents cited examples of how industry was already working on solutions. Themes include:

3.15.1 Building privacy concepts into devices and services from the beginning. This so-called "privacy by design" approach requires an early and detailed consideration of a full range of privacy issues and how they relate to and interact with other components of the IoT system, such as network security, resilience and user interface design;

3.15.2 Devising simpler terms and conditions for the collection and sharing of data, including the means to obtain informed consent from users via a range of innovative approaches; and

3.15.3 Related to simpler terms and conditions, many respondents supported the development of a common framework to simplify and categorise different levels of data sharing. For example, data sharing could be classified in three ways: unshared, shared only with the service provider or shared with everyone. Such frameworks should ideally take into account the type of data (e.g. personal or anonymised), given that not all types of data are equally sensitive. Several respondents also suggested that the framework should also seek to ensure the accuracy of shared data.

3.16 The suggestion of a common framework, in particular, would appear to have some merit, especially if it results in a clearer articulation of the risks and benefits to users from sharing their data as part of the IoT.

3.17 While many respondents supported the principle of a common framework, and some demonstrated evidence of some work on the subject, there was little evidence to date to suggest that various initiatives were converging on a single, standardised solution.

There could be a facilitating role for Ofcom in bringing together a common framework for data privacy

3.18 There is significant interest in the development of the IoT from a wide range of stakeholders across multiple industry sectors. This has the potential to cause co-ordination issues, which some respondents felt could inhibit the timely development of the IoT. In particular, co-ordination issues could occur:

3.18.1 Between stakeholders from different industry groups that traditionally have not worked closely together (e.g. the automotive and healthcare industries);

3.18.2 Between various government departments and regulatory authorities, with a set of often complementary public policy goals and duties; and

3.18.3 Between industry stakeholders and regulatory authorities, in the event that areas of responsibility are unclear.

3.19 A number of respondents noted that Ofcom could take on a co-ordinating role, working with industry, Government and other regulatory authorities to facilitate the

development of a common framework for data privacy. In particular, respondents acknowledged the important role of the Information Commissioner's Office (ICO) and recommended that Ofcom works closely with the ICO on matters of data privacy.

3.20 We see the merit in working with a range of stakeholders to better understand and potentially address issues of data privacy in the IoT. We note that Government and other agencies are already taking IoT-related activities. For example, in December 2014 the Government Office for Science published a review[6] by the Chief Scientific Advisor. This set out ten actions for the Government, including a proposal to work with stakeholders to define and agree best practice for information security.

Ofcom could also play a role in informing citizens and consumers about the benefits of the IoT

3.21 Given how important it will be for users to have trust and confidence in how their data will be used, many respondents identified a potential role for Ofcom in informing citizens and consumers about the benefits of the IoT. This would build upon our existing work in informing citizens and consumers about a range of communications issues, such as advice on the use of smartphone apps and on the cost to call non-geographic telephone numbers.

3.22 Any such information campaign would need to take into account different age groups' attitudes to sharing. For example, widespread use of social media could mean that younger users would be happier to share all of their IoT data, should they see the value in doing so, especially if they trust the brand of the devices or services used. Older users, on the other hand, may be less comfortable with sharing data without a fuller assessment of risks and benefits.

[6] Internet of things: making the most of the second digital revolution, Government Office for Science, 18 December 2014, https://www.gov.uk/government/publications/internet-of-things-blackett-review

Section 4

Network security and resilience

4.1 As the IoT develops it is likely that it will encompass an increasing number of services on which citizens and consumers come to rely. It will become increasingly important to ensure that the networks delivering these services are robust and reliable and that data is delivered over them securely.

4.2 This creates particular challenges as the traditional security approaches used in telecoms may not be applicable to the high volume, low cost devices likely to be used by many IoT services.

4.3 We have a function to ensure that certain networks and services meet minimum standards of security and resilience. Work is ongoing within industry to deliver secure and robust IoT networks and services, recognising that different services will have different requirements for security and resilience. We also recognise that some IoT services that have requirements for high levels of security and resilience could be deployed over private networks and that security and resilience obligations do not apply to private networks under current legislation.

4.4 Given our existing functions and the importance of the topic, we believe there is some merit in exploring whether we could play a co-coordinating or facilitating role to encourage the development of robust and flexible solutions.

4.5 We discuss these points in more detail below.

Some IoT applications will form part of the UK's critical national infrastructure

4.6 The diversity and scale of the IoT will lead to the proliferation of devices and services, many of which will be entirely new. A recent study[7] identified the significant market potential of the following categories of service (including the approximate predicted number of connections in the UK by 2022 in brackets):

4.6.1 **Intelligent buildings:** including the control of heating, ventilation and air conditioning (HVAC) systems, lighting, security and fire alarms, device remote control and remote locking of doors and windows (182 million);

4.6.2 **Utilities:** including remote metering and control of electricity, gas and water supplies and smart grid (59 million);

4.6.3 **Automotive:** including autonomous vehicles, security and tracking, road charging and insurance and traffic management (59 million); and

4.6.4 **Healthcare:** including health and fitness tracking devices, remote clinical monitoring and connected medicine dispensers (25 million).

[7] M2M Application Characteristics and their Implications for Spectrum, report for Ofcom, April 2014, http://stakeholders.ofcom.org.uk/market-data-research/other/technology-research/2014/M2MSpectrum

4.7 Different applications will have different requirements for network security and resilience. For example, a simple fitness monitoring device that tracks an individual's physical movement will not require a highly resilient network connection; if the device's network connection is interrupted the data can be resent when the connection is restored without significantly impacting the integrity of the application.

4.8 On the other hand, a smart grid service, that controls key components of the electrical generation system, will require a highly resilient network to ensure measurements and control messages are received and acted upon in real time. In addition, the smart grid network will need to be secure against malicious attack.

4.9 Many of the devices and services that are currently emerging fall into the former category, where the impacts of security flaws or temporary service interruptions are likely to be limited. However, we also expect services to emerge for which such failings would have more serious consequences and which will have correspondingly stricter requirements for security and resilience. In addition to smart grid, these are likely to include services to monitor or control transport infrastructure and building automation.

4.10 Most respondents noted the importance of security and resilience in IoT networks and services. Many respondents also highlighted the varied requirements of IoT services and emphasised that a simple, "one size fits all" solution would not be appropriate.

Regulations are already in place covering security and resilience of communications networks

4.11 The Communications Act 2003 (the "Act") places certain security and resilience obligations[8] on providers of publicly available[9] networks and services. These can be summarised as follows:

4.11.1 Network and service providers must take appropriate measures to manage risks to security, in particular to minimise the impact on end users and interconnected networks;

4.11.2 Network providers must take all appropriate steps to protect, so far as possible, network availability; and

4.11.3 Network and service providers must report to Ofcom breaches of security or reductions in availability which have a significant impact on the network or service.

4.12 Ofcom has corresponding powers to enforce these obligations, ultimately including the power to fine companies that do not comply. We issue, and regularly review, guidance[10] to network and service providers on what we expect them to do in demonstrating compliance. Through the UK Regulators Network[11], we also work with

[8] Sections 105A to D of the Act
[9] As set out in section 151 of the Act, a public communications service is one that is provided so as to be available for use by members of the public. A public communications network is one that is provided wholly or mainly for the purpose of making electronic communications services available to members of the public.
[10] http://stakeholders.ofcom.org.uk/telecoms/policy/security-resilience/
[11] http://www.ukrn.org.uk/

the regulators of other sectors to consider security and resilience issues with cross-sector implications.

4.13 We do not address IoT directly in the current guidance. The number and type of IoT services that could fall under the definitions of the Act are not currently clear. For example, a highly secure and resilient smart grid application might be deployed over a private network; security and resilience obligations do not apply to private networks under current legislation. A detailed assessment of how emerging IoT networks and services relate to the Act will be necessary as the IoT develops.

4.14 To the extent that IoT networks and services fall under the definitions in the Act[12], they would be covered by existing obligations. Much of our guidance stresses the importance of providers considering security and resilience in line with existing technical standards and industry best practice when designing and operating their products. We also note the use of the word "appropriate" in the legislation; the "appropriate" level of security or resilience may vary considerably between critical and non-critical IoT applications.

4.15 Many respondents believed that there was little evidence to support new, IoT-specific regulation on security and resilience, recommending instead the further development and application of existing regulations.

4.16 Several respondents explicitly linked the security of the IoT with ongoing Government and industry efforts to protect online services against malicious attack. Others emphasised that security and resilience issues are much broader, including:

4.16.1 Providers might choose to deliver IoT services that have strict security or resilience requirements using technologies that are unsuited for delivering these requirements. For example, a decision may be taken to implement a safety of life application at lower cost using a Wi-Fi connection, which operates in shared spectrum and can only provide a best effort service; and

4.16.2 The functionality of communications devices is increasingly implemented in software, as opposed to hardware. The main advantage for this is that functionality implemented in software can more easily be updated if performance enhancements or bug fixes are required. However, updating and maintaining large numbers of IoT devices could be a significant undertaking, especially if software cannot be updated remotely or an error occurs that requires a technician to make a site visit. Failure to maintain IoT devices with up-to-date software could disrupt IoT services through malfunctioning devices or illegal access to data.

There could be a facilitating role for Ofcom in bringing together a common approach for network security and resilience

4.17 A number of respondents noted that industry was aware of issues related to network security and resilience and work was underway to address them. There was, however, merit in a comprehensive yet proportionate approach which brings together a range of stakeholders to deliver secure and resilient IoT networks. Most

[12] The Act applies to providers of all "Public Electronic Communications Networks" (PECN) and "Public Electronic Communications Services" (PECS).

respondents expressed a strong preference for building upon existing regulations, rather than developing new, IoT-specific approaches.

4.18 There was a range of views on the role that Ofcom should play, given our existing duties for network security and resilience. In general, there was broad consensus that Ofcom should adopt a co-ordinating role, working with a range of stakeholders to facilitate a common approach for delivering secure and resilient IoT networks and services. Other views on specific roles for Ofcom included:

4.18.1 Developing guidelines for end-to-end performance and security of IoT services, perhaps leading to a set of minimum requirements;

4.18.2 Mandating pre-delivery testing of IoT devices to ensure that they are free of features of flaws that could compromise security or resilience;

4.18.3 Ensuring that manufacturers of IoT devices and service providers educate users of security and resilience risks and responsibilities; and

4.18.4 Ensuring that any steps taken to address security and resilience in IoT networks and services are co-ordinated internationally.

4.19 Given our existing duties and the potential for significant benefits delivered by the IoT, we see the merit in exploring whether Ofcom can play a facilitating role in in this area.

Section 5

Availability of spectrum for IoT networks

5.1 The majority of responses supported a view that spectrum availability will not be a barrier to the development of the IoT in the short to medium term. The low data rates typical of the majority of emerging IoT applications mean that they can be supported within existing allocations, including the 870/915MHz bands that Ofcom has made available.

5.2 However, the spectrum requirements for the IoT in the longer term are uncertain. The market is currently immature and future generations of IoT applications might have increased demands for spectrum (for example, if significant demand for high data rate video emerges). It will be important, therefore, to continue to monitor the development of the IoT to predict any significant changes in spectrum demand.

5.3 Respondents emphasised that international harmonisation of spectrum and standards is also likely to be vital for delivering economies of scale and lower cost consumer equipment; given the need for very low cost equipment for some applications, this will be particularly important for the longer term success of the IoT.

5.4 We discuss these points in more detail below.

IoT networks will use a range of technologies and spectrum bands

5.5 In our call for input we set out our view that, given the likely diversity of applications and devices, a range of technologies and spectrum bands would be used to deliver IoT services. The framework in Figure 4 illustrates the factors that may influence spectrum requirements, including:

5.5.1 Whether wide area or deep in-building coverage is required, suggesting the need for lower frequency spectrum;

5.5.2 Whether a degree of service availability and quality is required, which suggests a preference for licensed spectrum; and

5.5.3 Whether there is a need for devices to have a long battery life, suggesting a preference for networks based on lower complexity, IoT-optimised technologies which may benefit from their own allocation of spectrum.

5.6 There was broad agreement from respondents that a range of technologies and spectrum bands would be required to support the IoT. In addition, many respondents noted the complementary nature of licensed and licence exempt access to spectrum and that access to spectrum on a shared basis will become increasingly important for a range of services, including the IoT.

5.7 Respondents acknowledged that some IoT devices will use common, general purpose technologies. For example, consumer IoT devices that operate over short ranges, such as health or fitness trackers, do not typically require highly reliable, real time communication. These applications are likely to use technologies such as Bluetooth and Wi-Fi, which transmit on a licence exempt basis.

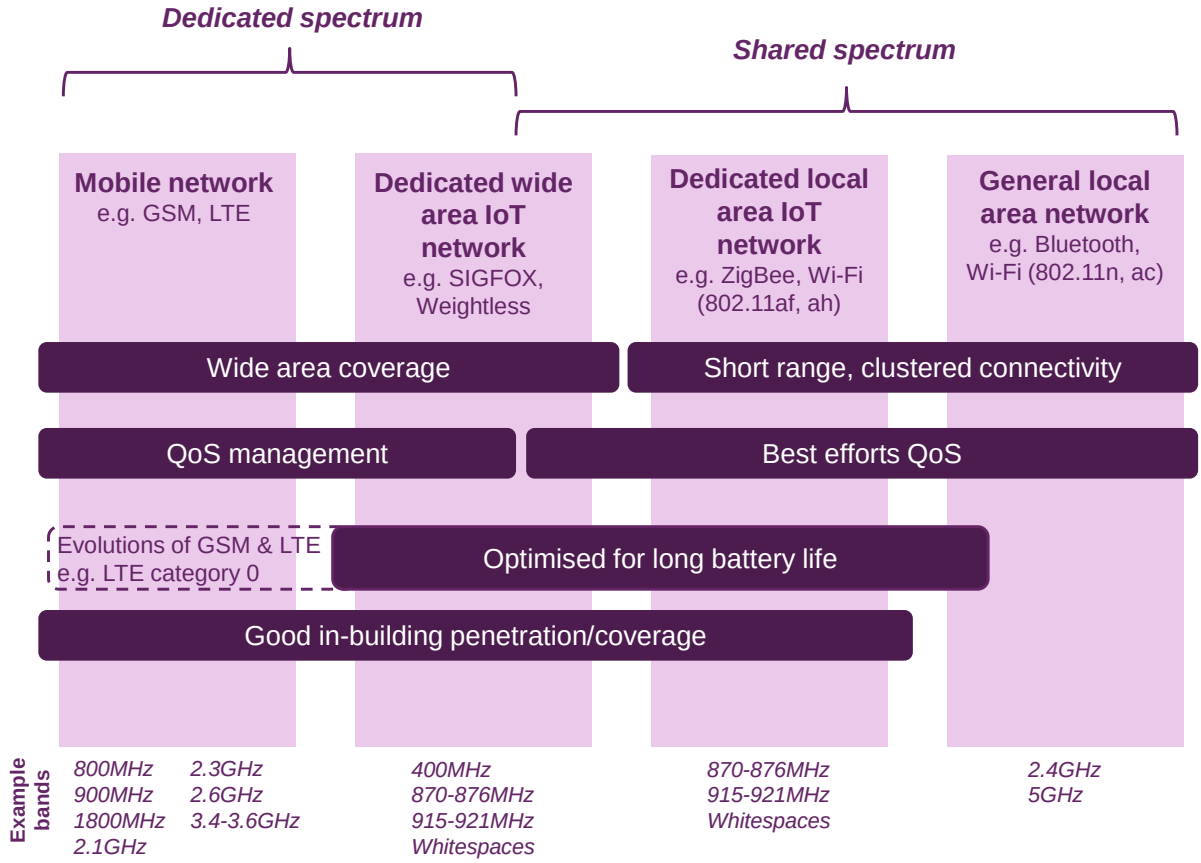


Figure 4: Framework for considering spectrum requirements for the IoT

5.8 In some cases, these technologies are evolving to better support the particular requirements of the IoT, such as lower data rates and power consumption. For example, many devices already support low power Bluetooth Smart and an IoT-optimised version of Wi-Fi, called 802.11ah, is being developed.

5.9 Over longer ranges, respondents acknowledged the roles of both bespoke IoT networks and mobile networks that have been adapted or optimised for IoT use. Respondents typically focused their support on one of these approaches and numbers of respondents supporting each was broadly equal.

5.10 Bespoke IoT networks offer the potential for very efficient operation, as they have been designed to meet the specific requirements of IoT services (as opposed to the broader set of requirements for general consumer data services). In particular, bespoke IoT network technologies have been designed to support very low cost devices and low data rate communications.

5.11 Bespoke IoT network technologies can operate using spectrum either on a licensed or licence exempt basis. In the case of licence exempt operation, this flexibility makes it possible to deploy bespoke IoT networks without the need for spectrum licences, potentially reducing barriers to entry for new network operators. The 870MHz frequency band, which has recently been made available in the UK, is one option for deploying IoT networks on a licence exempt basis.

5.12 One potential disadvantage of using bespoke IoT technology is that this will typically involve deploying entirely new network equipment. On the other hand, and especially if communication over longer ranges is an application requirement, IoT-optimised

mobile networks could be, in principle, more easily and cheaply deployed by reusing components from the existing mobile network. As a result, there are a number of ongoing activities which are seeking to enhance mobile network technologies to efficiently support IoT services. They include:

5.12.1 An enhancement to technology used in 4G networks to support lower data rates and less complex user devices (so-called LTE category 0);

5.12.2 An enhancement to the technology used in 2G mobile networks to support very low data rates and device complexity while using the same spectrum allocations as mobile networks (so-called GERAN[13] Release 13); and

5.12.3 In the longer term, 5G mobile networks may be designed to efficiently support a range of services, including IoT traffic.

5.13 In addition, three respondents noted the role of satellite communications to deliver IoT services, especially in very rural or remote areas where coverage from terrestrial networks is uneconomical or impractical. Satellite delivery could also be appropriate where there is the potential for connectivity with terrestrial networks to be affected by natural events, such as floods or earthquakes. A smaller, lower cost type of satellite, known as a micro- or nano-satellite, is emerging that may be suited to delivering IoT services.

5.14 A common theme through many responses was the recognition that the IoT would not consist of a single network or technology; rather, it would be a heterogeneous collection of technologies operating on both a licensed and licence exempt basis. Most respondents emphasised the need for open and interoperable standards.

Spectrum availability is unlikely to be a barrier to the development of the IoT in the short-medium term

5.15 While spectrum is a key enabler for the IoT, few respondents suggests that its availability would be a barrier to the development of the IoT in the short to medium term. Respondents cited reasons including:

5.15.1 The IoT is expected to grow to comprise hundreds of millions of devices in the UK alone. However, in many cases the amount of data expected to be exchanged by each device is expected to be very small, perhaps a low as several hundred kilobytes per device over the course of a day. One respondent noted that by 2018 IoT devices are expected to make up 47% of worldwide connected devices, while supporting only 3% of traffic; and

5.15.2 Recent initiatives have made additional spectrum available for a range of uses, including the IoT. These include licence exempt access to the bands at 870 and 915MHz and the proposal to allow high duty cycle network relay stations to operate on a light licensed basis in the 870 – 873MHz band. In addition, we are exploring with mobile network operators options for modifying the terms of their licences to allow the deployment of IoT-optimised technologies within their existing spectrum allocations.

[13] GERAN is the GSM EDGE Radio Access Network, a name given to the radio part of a 2G mobile network.

5.16 A number of respondents supported Ofcom's stance in proactively opening up licence exempt access to the 870 and 915MHz bands, with some stakeholders requesting that we encourage regulatory authorities in other countries to follow suit.

5.17 Respondents also noted that the bands currently used to deploy mobile broadband networks could also be used for IoT networks; these range in frequency from the 800MHz band, which is currently used for 4G services, to bands above 2GHz, which are currently used for both 3G and 4G services. Additional spectrum will become available for mobile broadband services by early 2016 following the award of the 2.3 and 3.4 – 3.6GHz bands and this spectrum could also potentially be used for IoT services.

5.18 Several respondents mentioned that certain applications, in particular those operating indoors and over short ranges, could use the existing allocations at 2.4 and 5GHz on a licence exempt basis. These bands are used by a range of services and technologies on a shared basis, including Wi-Fi and Bluetooth, on condition that interference is not caused to other spectrum users.

Additional spectrum may be required in the longer term as the IoT matures

5.19 Several factors suggest that, in the longer term and as the IoT matures, additional spectrum may be required. For instance:

5.19.1 Later generations of IoT device may evolve to transmit greater volumes of data, for example, if significant demand for video-based IoT services emerges; and

5.19.2 It is challenging to predict accurately the exact size and nature of the future IoT and its requirements for spectrum in the longer term.

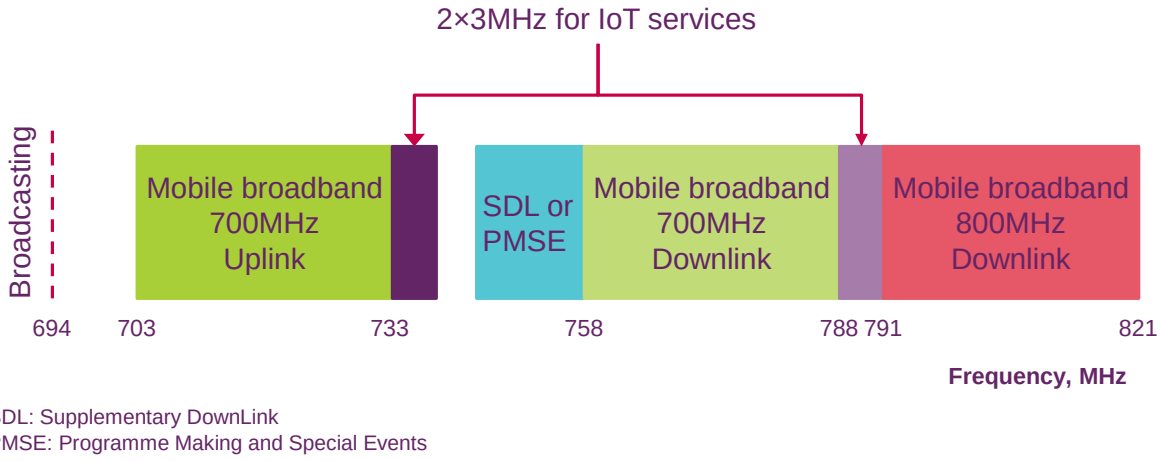
5.20 Respondents made a number of suggestions for how future demand for additional capacity might be met. Three common suggestions were an allocation for IoT as part of any future release of spectrum at 700MHz for mobile broadband; additional spectrum for licence exempt use below 1GHz; and greater use of spectrum on a shared basis. We cover each in more detail below.

IoT allocation at 700MHz

5.21 CEPT[14] is currently considering a proposal to allocate spectrum at 700MHz for IoT services. This spectrum could be used by IoT-optimised mobile technologies, such as that being developed in GERAN Release 13.

5.22 The proposal is to allocate 2×3MHz as part of the duplex gap for any future allocation at 700MHz for mobile broadband services. A working group within the CEPT is carrying out studies on the use of the bands 733-736MHz and 788-791MHz for machine to machine and IoT communications, as illustrated in Figure 5. In our view there would be benefit in harmonising spectrum for this application.

[14] The European Conference of Postal and Telecommunications Administrations (CEPT) is a coordinating body. Within CEPT, the Electronic Communications Committee's (ECC) working group PT1 is responsible for implementing technology and service neutral rules for mobile and fixed communications networks.



SDL: Supplementary DownLink
PMSE: Programme Making and Special Events

Figure 5: Spectrum around 700MHz under study for machine to machine and IoT communications

5.23 There was broad support from respondents for the proposal to allocate spectrum at 700MHz for future IoT services. In particular, this approach has the potential for international harmonisation, delivering a range of low cost devices for IoT services. In addition, the use of sub-1GHz spectrum is particularly suited to delivering services over longer ranges and deep into buildings.

5.24 We recognise that the IoT will be delivered by a range of technologies and network architectures. We therefore support a study on the technical feasibility of the use of spectrum at 700MHz as one of several IoT options, noting that it has some stakeholder interest, including from network operators and equipment manufacturers. One potential spectrum efficiency benefit is that it could exploit what would otherwise be a relatively sterile gap between the 700MHz and 800MHz downlink bands.

5.25 A key proviso is that technical studies would need to be followed by evidence of an IoT allocation being a valuable prospective use of this spectrum (and more valuable than other prospective uses) before we would be persuaded to support a harmonisation measure.

Additional spectrum below 1GHz for licence exempt use

5.26 While the availability of the 870 and 915MHz bands was broadly welcomed, several stakeholders also highlighted the potential need for additional spectrum below 1GHz for licence exempt use. As with the above proposed allocation at 700MHz, respondents viewed spectrum below 1GHz as particularly attractive given the ability to provide coverage over long ranges and deep into properties.

5.27 Respondents suggested that this additional bandwidth could be found either by identifying and clearing bands for use, or by relaxing technical conditions on the use of bands that are already available so that they can be accessed by a greater range of devices.

5.27.1 *Clearing new bands for use:* There was no clear consensus on which specific bands below 1GHz would be particularly suitable, although one respondent suggested that at least 20MHz of bandwidth would be required.

Several respondents acknowledged the potential to use white space[15] spectrum for a range of IoT services and noted that services are already being piloted around the country. Another respondent suggested that additional spectrum should be made available between 400MHz and 1GHz, emphasising that licence exempt access to spectrum offers attractively low barriers to entry for new network and service providers; and

5.27.2 *Relaxing technical conditions:* Several respondents noted that there are a number of bands below 1GHz that are available on a licence exempt basis but are subject to technical conditions that limit the technologies or applications that can be deployed within them. These could include, for example, bands currently designated for "short range devices", such as the 868MHz band. One respondent suggested the potential benefit in changing technical conditions, ideally on an internationally harmonised basis, to allow devices to transmit at a higher power and duty cycle. On the other hand, another respondent cautioned against such changes as they might increase the potential for interference with services operating in neighbouring spectrum bands.

5.28 We remain committed to seeking liberalisation opportunities, while ensuring the efficient use of spectrum for all users. To that end we are actively engaged in the ongoing work of CEPT[16] SE24, which is expected to be completed in the autumn of 2015.

5.29 Several respondents expressed a view that licence exempt access to spectrum would be an attractive option for initial network deployments. However, in the longer term, and as the number of networks sharing the licence exempt spectrum increases, respondents suggested that operators might choose to migrate to licensed spectrum, where it may be easier to manage quality of service.

5.30 Similarly, another respondent cautioned against making too much spectrum available on a licence exempt basis, as it may be difficult to migrate to a licensed approach should this subsequently become necessary.

5.31 On spectrum availability more generally, several respondents acknowledged the challenge in accurately predicting demand for IoT services in the longer term. They recommended that we monitor the development of the IoT and to continue to refine assessments of future spectrum demand, in particular in preparation for future World Radiocommunications Conferences[17] (WRCs).

Greater use of spectrum on a shared basis

5.32 Some IoT applications may only transmit a small quantity of data, infrequently and at specific locations. IoT applications with such characteristics have the potential to

[15] "White spaces" is the name given to parts of spectrum that are unused in a particular location and time. White space technology is now being piloted in the UK, using white spaces that exist between digital terrestrial TV broadcasting transmissions (470 to 790MHz).
[16] The SE24 group within CEPT is a spectrum engineering working group that specifically studies short range devices.
[17] The International Telecommunications Union (ITU) meets to amend the radio regulations that govern international use of spectrum at World Radiocommunications Conferences, which typically take place every three or four years.

share spectrum that would otherwise be underused, or unused, at particular locations and times.

5.33 Several respondents noted the complementary role that access to spectrum on a shared basis can play alongside other spectrum access approaches. In particular, these respondents supported the adoption of Licensed Shared Access (LSA). Broadly, the LSA concept aims to open up access to spectrum bands where this spectrum cannot be fully cleared but is not being used in all locations or at all times.

5.34 On sharing more generally, however, several stakeholders argued that access to spectrum on shared basis should only be considered if existing users can be protected from interference.

5.35 On balance, respondents broadly supported our view[18] that the nature of some IoT applications might make them particularly suited to delivery using spectrum that is shared with other services.

[18] The future role of spectrum sharing for mobile and wireless data services - Licensed sharing, Wi-Fi, and dynamic spectrum access, April 2014, http://stakeholders.ofcom.org.uk/consultations/spectrum-sharing/statement/

Section 6

Telephone number and address management

6.1 Broadly, responses from stakeholders suggested that the availability of network addresses, including telephone numbers and internet addresses, will not be a barrier to the development of the IoT.

6.2 There are a range of options for assigning addresses to IoT devices and the choice of address may depend on factors including type of application and the network technology used. An additional factor is whether there is a need for access to the wider internet, which may suggest that the use of Internet Protocol version 6 (IPv6) addressing in the longer term is necessary.

6.3 We summarise key points from stakeholders' responses below.

There are a range of options for identifying and addressing IoT devices

6.4 Any device that connects to a communications network requires an address that:

6.4.1 Uniquely identifies it and differentiates it from other devices on the network;

6.4.2 Can be used to route traffic to the device; and

6.4.3 Can be used to identify the sender of data received by a device on the network.

6.5 There are many address formats that can be assigned and the choice of format will depend on a number of factors. For IoT devices, relevant factors include:

6.5.1 Whether the application supported by the device requires limited connectivity with devices within the same network, or wider connectivity with devices on other networks or the internet; and

6.5.2 The technology or network type to which the device is attached.

6.6 There was a general view across the range of responses that a single addressing format for IoT devices was not necessary, recognising the diversity of applications, technologies and devices that could comprise the IoT. In addition, some respondents believed that the choices of address format could change over time as application requirements of technologies change.

6.7 The majority of responses focused on two addresses, namely telephone numbers and internet addresses. We summarise key points from stakeholders' responses below.

Mobile telephone numbers

6.8 Devices connected to mobile networks, such as smartphones or tablets, use a number of addresses and identifiers. Most of these addresses are hidden from users,

such as the number used to identify the SIM[19] card within the device or the number used to uniquely identify the device itself. The telephone number when used to communicate by voice or data messaging, on the other hand, is known by and familiar to users, who find it intuitive to use.

6.9 It is sometimes assumed that any IoT device connected to a mobile network will also require its own, unique telephone number. This can cause a concern that the expected large volume of IoT devices could put pressure on the limited supply of available telephone numbers, in particular mobile numbers. In some countries, the national regulatory authority has sought to manage this by allocating a range of telephone numbers specifically for IoT applications.

6.10 However, the allocation of a telephone number is not necessary for IoT applications; by their nature, IoT applications will involve communication between devices, rather than humans, so an intuitive and recognisable telephone number is not required. In principle, device or SIM-level addresses can be used as an alternative.

6.11 Our current position, as set out in our call for input, is that IoT devices are unlikely to need to use mobile telephone numbers to the extent that this would put pressure on number availability. Broadly, the majority of respondents agreed with this position and supported our intention to monitor the use of telephone numbers by devices as the IoT develops. One respondent suggested that, if necessary and supported by evidence of number scarcity, we should allocate a range of numbers for IoT devices. We also highlight that in some of the cases where telephone numbers are required and the service remains on the same network, it may be possible to use Internal Routing Codes which can be used independently by all networks.

6.12 Several respondents commented on the need to assign unique addresses to SIM cards for IoT devices in such a way that does not inhibit national allocation to mobile broadband devices more generally[20]. One respondent, an international mobile network operator, noted that they already allocate SIM identifiers from an international pool, which does not impact upon their country-specific pools. We would support consideration of international numbering resources where the service is to be used primarily abroad.

Internet addresses

6.13 Assigning internet protocol (IP) addresses to IoT devices affords significant scalability, as it enables the creation of both small and large networks. In particular, it facilitates the interconnection of multiple networks to create much larger networks, such as the global internet.

6.14 Not all IoT applications will require connectivity with the wider internet. However, there may be some benefits in still using IP addresses for smaller, private networks, including the ability to take advantage of low cost, commonly available networking equipment or the opportunity to easily scale up the size of the network should this subsequently be required.

6.15 The most common format of IP address is known as an IPv4 address. The principal limitation of this format is the size of its address space, i.e. the number of unique

[19] Subscriber Identity Module, the integrated circuit printed on a small card and installed within a mobile device to uniquely identify the subscriber on the network.
[20] SIM identification numbers include a component that identifies the assigning, or home, country.

addresses it can generate is limited to approximately 4.3 billion addresses. Technical advances and network engineering solutions have increased the number of devices which can be connected by effectively allowing devices within private networks to use a common set of private addresses and still appear to the rest of the internet to have a unique address. However, the desire for a more scalable solution has contributed to the development of a new version of the Internet Protocol, known as IPv6. One component of IPv6 is an address format with a significantly increased address space.

6.16 Network operators are in the process of migrating their networks to support IPv6 connectivity. We recently undertook a study[21] into utilisation of IPv6 by UK networks and it is our understanding that most major retail ISPs will start to roll out IPv6 connectivity to their customers during 2015.

6.17 In our call for input, we sought views on whether support for IPv6 would be necessary for the development of the IoT. Broadly, the majority of respondents acknowledged the important role that IPv6 will play, particularly in the longer term. Many respondents emphasised the importance of operators migrating their networks to support IPv6. However, a number of respondents also noted that not all IoT applications would require global internet connectivity (and therefore would benefit from an IPv6 address) and that some applications could use alternative address formats.

6.18 On balance, we do not believe that IP address availability will be a barrier to the development of the IoT. In the short to medium term, the subset of IoT applications that require internet connectivity can be supported using IPv4 addresses with appropriate network translation or application gateway. In the longer term, as demand for IPv6 support increases and operators continue to upgrade their networks, IPv6 will become available to support the operation of the IoT where necessary.

[21] Study into IPv4 and IPv6 allocations, December 2014, http://stakeholders.ofcom.org.uk/binaries/research/technology-research/2014/rtfm.pdf

Section 7

Conclusions and next steps

7.1 In this section we set out our conclusions and proposed next steps, grouped into key themes, based on responses to the call for input and our own analysis. Some of these themes are a good fit with Ofcom's existing duties, while for others there is the potential for us to play a facilitating role in seeking collaborative outcomes.

Data privacy and consumer literacy

7.2 On balance, respondents indicated that data privacy had the potential to be the greatest single barrier to the development of the IoT. In particular, respondents were concerned that a lack of trust on the part of citizens and consumers could impact upon their appetite for sharing personal data, which could in turn constrain the benefits that the IoT could deliver.

7.3 We also note that privacy concerns in relation to the IoT have been raised more broadly. For example, in their recent report[22] on the IoT the Government identified their intention to work with industry and other partners on data privacy matters. We are also aware that the Competition and Markets Authority (CMA) has initiated a call for information on the commercial use of data, aspects of which have relevance to data privacy within the IoT.

7.4 We note that in the UK the Information Commissioner's Office (ICO) has the primary duty for data privacy issues. We also acknowledge that a number of respondents suggested that Ofcom should take on a co-ordinating role, working with industry, Government and other regulatory authorities to facilitate the development of a common framework for data privacy.

7.5 We therefore propose to work with relevant organisations, primarily the ICO, to identify and explore solutions to data privacy issues in the IoT, in which Ofcom will play a facilitating role. We expect that this work will have both national and international dimensions.

7.6 On an international level, we propose to contribute to IoT-related work streams within relevant European agencies, such as BEREC. In the first instance, this will involve contributing to BEREC's ongoing activity on the implications of the IoT and machine-to-machine communications.

7.7 On a national level, we propose to undertake preliminary work, in collaboration with the ICO, Government and other stakeholders, specifically to understand the detailed nature of potential data privacy issues. On the basis of this work, we propose to identify key components of an approach or framework for data privacy for wider input from industry. This could include:

7.7.1 An assessment of the extent to which existing data protection regulations fully encompass the IoT;

[22] The Internet of Things: making the most of the second digital revolution, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/389315/14-1230-internet-of-things-review.pdf

7.7.2 A set of principles for the sharing of data within the IoT, such as ensuring that only the minimum amount of data for a given application is collected and limiting the time that data may be stored;

7.7.3 Exploring the need for work to better understand consumer attitudes to sharing data and approaches to providing consumers with the necessary information to enable them to make an informed decision on whether to share their data; and

7.7.4 In the longer term and as the IoT develops, exploring the merit of a consumer information campaign to highlight the potential benefits of the IoT.

Network security and resilience

7.8 As the IoT develops and encompasses an increasing number of services on which citizens and consumers come to rely, it will become increasingly important to ensure that the networks delivering these services are robust and the data delivered over them is secure. This creates particular challenges as the traditional security approaches used in telecoms may not be applicable to the high volume, low cost devices likely to be used by many IoT services.

7.9 We note that work is ongoing in industry to deliver secure and robust IoT networks and services. However, given the importance of the topic and our existing duties in this area, we believe there is some merit in considering how best it should be reflected in our existing security and resilience guidance. Also, where gaps in existing standards and best practices of relevance to the IoT are identified, we will explore taking a co-coordinating or facilitating role to encourage the development of robust and flexible solutions.

7.10 Regulations are already in place which cover security and resilience of communications networks generally. These regulations place certain security and resilience obligations on providers of publicly available networks and services. Ofcom has corresponding powers to enforce these obligations and we regularly review our guidance to network and service providers on what we expect them to do in demonstrating compliance.

7.11 We will undertake work to consider the impact of IoT on our existing security and resilience guidance and whether this needs updating as a result. We believe that our existing overall approach of encouraging providers to consider security and resilience in line with established standards and best practice will be remain the correct one in the IoT domain. However, it may be that we need to reference additional IoT-specific standards, or note the need for new ones where none currently exist.

7.12 As specific gaps in the existing approaches are identified, we will coordinate with other stakeholders to develop standards and best practice relevant to the IoT. Existing national and international groups drawing on industry and government experts are expected to be the focus for any required technical work. We note the comments we have received that this is more likely to be about extending the scope of existing approaches rather than creating entirely new standards and regulation. We will also be mindful of limitations of our powers in this area, which are focussed on securing networks and services.

7.13 We will continue to work closely with government colleagues on relevant issues, such as implementing the UK's Cyber Security Strategy and ensure relevant links to the IoT are made.

Availability of spectrum for IoT services

7.14 Responses to our call for input underlined our existing view that spectrum will be an important enabler to the IoT. Ofcom has a duty to manage use of spectrum in the UK and we have already taken steps to assess the spectrum implications for the IoT.

7.15 We conclude that the availability of spectrum will not pose a barrier to the development of the IoT in the short to medium term. The low data rates typical of the majority of emerging IoT applications mean that they can be supported within existing allocations. In addition, we have taken steps to make additional spectrum available for IoT services, such as the 870/915MHz bands, and are exploring options for liberalising licence conditions on mobile spectrum use to support the IoT.

7.16 However, the spectrum requirements for the IoT in the longer term are uncertain; the market is currently immature and future generations of IoT applications might have increased demands for spectrum.

7.17 The international harmonisation of spectrum and standards is also likely to be vital for delivering economies of scale and lower cost consumer equipment; given the need for very low cost equipment, this will be particularly important for the longer term success of the IoT.

7.18 We propose to continue our existing approach to identifying and making available spectrum for use by the IoT. This will involve:

7.18.1 Providing information to stakeholders about the bands that are currently available for IoT use. A list of bands that could be used for the IoT is included for information in Annex 1;

7.18.2 Tracking the developing size and nature of the IoT through existing information gathering processes, such as the Communications Market Report and the Infrastructure Report; and

7.18.3 Continuing our periodic monitoring of licence exempt spectrum use in a number of bands used by IoT devices. This will enable us to identify at an early stage whether congestion and interference is likely to occur.

Telephone number and address management

7.19 We believe that limits on the availability of telephone numbers will not be a barrier to the development of the IoT as a range of alternative identifiers, such Internal Routing Codes, SIM or equipment identifiers and IP addresses could be used. We also consider that migration to IPv6 in the longer term is likely. This position is supported by our own recent monitoring of IPv6 migration, which was published in the recent Infrastructure Report.

7.20 We propose to continue to monitor use of, and demand for, telephone numbers and network addresses by IoT devices. This will include monitoring of the ongoing migration of support for IPv6 by internet service providers in the UK. We will continue

to be mindful of the limited supply of mobile telephone numbers and support the use of alternative addresses and numbering where appropriate.

Annex 1

List of possible bands for IoT applications

A1.1 There are already a number of spectrum bands which are suitable for deployment of IoT applications. These include:

1.1.1 Spectrum recently made available by Ofcom in the bands 870 – 876 MHz and 915 – 921 MHz[23];

1.1.2 A subset of licence exempt bands (see below for more details);

1.1.3 A subset of bands currently used for Business Radio and Fixed Links. The bands that may be used can be found by searching the UK Plan for Frequency Authorisation (UKPFA)[24] for licences for Business Radio (technically assigned) and Fixed Links (scanning telemetry); and

1.1.4 Unused spectrum between 55 and 68 MHz. Ofcom will consider requests for use of this spectrum on a case-by-case basis.[25]

A1.2 In the future, IoT applications could also be deployed in white spaces, which is the name given to parts of spectrum that are unused in a particular location and time. White space technology is currently being piloted in the UK, using white spaces that exist between digital terrestrial TV broadcasting transmissions (470 to 790 MHz).

Licence exempt bands suitable for IoT applications

A1.3 Several bands where licence exempt use is possible can also be used for IoT. The list below details the licence exempt applications that are potentially relevant for IoT use. For details of the bands where such applications are in use please refer to the UKPFA.

- Non-specific short-range devices
- Industrial/Commercial Telemetry and Tele-command
- Databuoy Telemetry
- Active Medical Implants
- Animal Implantable Devices
- Medical and Biological Applications

[23] See http://stakeholders.ofcom.org.uk/binaries/consultations/short-range-devices/statement/statement.pdf and http://stakeholders.ofcom.org.uk/binaries/consultations/network-relay-points/statement/NRP_statement.pdf

[24] See http://spectruminfo.ofcom.org.uk/spectrumInfo/ukpfa

[25] See http://stakeholders.ofcom.org.uk/spectrum/spectrum-awards/prospective-awards/award_55/

- Wideband Data Transmission Systems
- Wireless Access Systems (WAS)
- Short Range Indoor Data Links
- Railway Applications
- Devices for locating victims in distress or at risk
- Radio determination applications
- Radio Frequency Identification
- Road Transport and Traffic Telematics and Intelligent transport Systems including safety-related uses
- Inductive Applications
- Metal Detectors
- Alarms
- Social Alarms
- Vehicle Paging Alarms
- General Alarms Associated with Marine Applications Including Fixed Shore Installations
- Mobile, Transportable and Lone Worker Safety Alarms
- Fixed Alarms
- Model Control
- Radio Microphones
- Assistive Listening Devices
- Wireless Audio Applications and Low power FM transmitters
- Video Distribution for Private Use
- Radar Level Gauges
- Tank Level Probing Radar (TLPR)
- Automotive Short Range Radar