Representing:

Organisation

Organisation (if applicable):

Dixons Carphone

What additional details do you want to keep confidential?:

No

If you want part of your response kept confidential, which parts?:

Ofcom may publish a response summary:

Yes

I confirm that I have read the declaration:

Yes

1. IoT definition, applications and demand:

We would define IoT as any connected device other than mobile or tablet and PC.
Within IoT, we see a number of main verticals: home, transport, health, buildings, industry.
Within the smart home, the most relevant sector to us, we see the main sub-categories: security, entertainment, utilities, health.

From the research we have done it is clear that there is no consensus on the potential size of the market or the relative growth between categories, although we expect significant opportunity within the smart home, initially through smart energy management and entertainment controls, but expanding into other areas of home automation and control.

2. Spectrum requirements :

IoT technology may be divided into devices used indoors and those used outdoors. Those used indoors are likely to be connected on home broadband though some connectivity with outdoor mobile network may be desirable. The indoor devices are also likely to have connection to the mains power source allowing for a much higher transmit power and frequency of packet transmission.

Those devices used outdoors are likely to need a type of mobile network for their communications. If the devices are battery powered, the requirement will be to last anything between 1 to 10 years. In such a case the likely transmit power used must be limited. In order to achieve this, data packets sent cannot be too large or too frequent, while upload speed must be relatively low.

Regular mobile networks e.g. O2, EE etc. may not be ideal for this type of devices given the high spectrum frequencies they operate in, even if those are below 1GHz. Also there is a need to avoid regular Location Update messages as well as power control to avoid the near-far problem. The modulation used in 3G WCDMA or OFDM used in 4G may be quite a burden on limited power source. If mobile networks want to provision this type of connectivity, a whole new network infrastructure maybe required using simpler modulation and transmission techniques. The networks must also be given access to new lower frequency spectrum to reduce infrastructure costs and allow for far reaching of data packets.

Regular mobile networks are perfectly capable of handling traffic of the automotive M2M (Machine to Machine) nature, where the purpose is that of reporting on aspects of the car functionality i.e. the engines, tyres pressure, etc. given power source will not be a bottle neck. In-car entertainment systems will increasingly rely on some form of M2M connectivity (or an additional SIM card linked to user's account) transmitting over the mobile networks.

We can't however flood the network with every piece of generated data. We need a different network architecture and hierarchical architecture to manage this and avoid quality of service degradation. Ofcom should provide guidance on the optimum spectrum available.

It is very desirable that regulatory constraints do not have an adverse impact on implementation cost or power efficiency, given the need for low power and low cost requirements in many sensory devices.

3. Network-related issues:

Please see also the Spectrum section.

It would be desirable for Ofcom to take an active role in enabling only one IoT standard to become dominant. This would make it much easier for device interoperability and avoiding customer confusion about which device to buy that would function with their existing system.

Quality of service and repair SLAs (Service Level Agreement) within the IoT network including any broadband must be guaranteed such that consumers can always access their home devices. For example, access to home may be prevented if a part of the network goes offline and the Smart-lock at the front door become inoperable. Similar situations can occur for control of window locks and other safety elements at home reducing at home safety and security. Uninterrupted quality of service is imperative for IoT to be successful, so Ofcom should take an active role in ensuring this network resilience through ensuring adequate guarantees and SLAs are in place for the underlying infrastructure.

4. Security and resilience:

The regulator needs end to end responsibility for the security of IoT: hardware, software, solutions, applications, OS, user/consumer awareness and education, physical environment, roles and responsibilities in IoT; law enforcement and compliance monitoring.

We see IoT quickly becoming part of the CNI (Critical National Infrastructure) as it has the ability to impact on the national security and economy of the UK. A dedicated mobile network could be desirable to ensure separation from non- IoT traffic as availability of this network is likely to have a different availability risk assessment to the regular mobile network and tighter security.

Dixons Carphone is a great point at which to educate users about the privacy and security implications of these technologies. The human is always the weakest point in any security plan and the consumer must and will have responsibilities to the security of their own data and services. In order for the consumer to discharge those responsibilities they must be aware of them. Those responsibilities must be minimised to ensure a good customer experience and so someone or something must take up the shortfall in security tasks.

A managed IoT service for users to sign up to that gives some basic protection would be advisable as users are unlikely to update devices and software regularly e.g. update anti-virus, Windows or phone software. This lack of protection could put the entire network at risk.

Some element of responsibility will need to be removed from consumers if this network is to remain secure. Indeed, it would be preferable to keep all consumers out of this network, only allowing qualified technicians/companies to operate devices/software on it with consumers having access only to the soft interface on the front end of IoT devices for their options.

A regulator needs to be responsible for looking for and managing vulnerabilities in software and devices and putting minimum standards in place.

5. Data privacy:

Ofcom could play a role with regards to customer education. For example, customers should be made better aware of how to protect their data, passwords and devices. Concern over data privacy and security represents one of the major barriers to IoT adoption, so there is a need for significant investment in education, training and technical support to overcome these concerns and facilitate the growth of the IoT.

Ofcom could provide self-assessments to companies in order to check the products against official industry standards set by Ofcom for which in return Ofcom provides accreditations. This could be similar to energy efficiency labels seen nowadays on electric appliances, ranking IoT devices in terms of risk / security. For example, companies could register products on an official Ofcom register after applying self-assessments. Failures to apply to Ofcom standards could lead to the removal of the seal of approval and could also lead to fines in cases where these seals are used to miss-lead customers.

Ofcom could also help to support the wider industry with regards to the UK Data Protection regulator (ICO). They could help by educating the ICO to understand the issues around the IoT, better explaining the difficulties the industry is facing.

Ofcom could create an industry forum which is used to discuss the wider implications of IoT to companies signing up to the forum; allowed to use an official Ofcom label on their websites in order to reflect the support and engagement these companies offer to Ofcom.

Another good tool would be for Ofcom to provide free audits for companies that would like self-assessments validated by the regulator. (Passed or validated assessments could lead to a star rating for companies)

In terms of personal data, it is imperative that there are boundaries set for the industry as whole on what can and cannot be done with personal data gathered from all IoT devices. Soon these devices will gather personal data ranging from presence at home to various behaviours and type of living whether healthy or otherwise. Clarity of data regulation is required to ensure that this data is not used without permission from the customer, with certain sensitive information not allowed to be used at all.

6. Numbering and addressing:

IPv6 should finally become the norm to allow for much needed IP addresses. Even though initially many IoT devices may be on an internal network thereby allowing them to have access to the full spectrum of IP addresses, were they to have a dual connectivity function of indoors and outdoors, it would be very important to have access to the necessary IP addressing pool to accommodate the millions of devices predicted to come online in the next 10 years.

From Ofcom's own document: MC/111 Internet Protocol Version 6 Deployment Study, the report finds that by any measure, the UK lags behind its peers in IPv6 deployment. IPv4 address exhaustion and a failure to transition to IPv6 has a significant impact on innovation as it is the essential building block for any technology that connects to the Internet. Failure to keep up with competitor economies will have an impact on the UK's consumer access to broadband, on eGovernment, intelligent highway systems, sensor technologies, mobile Internet applications, distributed generation of renewable energy, remote and automated monitoring of natural resources, and support for advanced employment, immigration and welfare applications.

According to said report, out of the 51 UK broadband access service providers listed on ThinkBroadband website, only six provide some form of IPv6 service. These six do not include the UK's largest broadband providers such as BT, Sky and Virgin Media.

7. Devices:

Please see the Spectrum section

8. Digital literacy:

According to the Ofcom Communication Market report 2014, internet take-up for the UK rose two percentage points to 82% between Q1 2013 and Q1 2014, but take-up varied by age, gender and socio-economic group.

There is need for consumers to have a better understanding of the internet in terms of advantages and threats such as hacking and Ofcom is well placed to sponsor this learning activity, partnering with relevant companies across the IOT value chain. Rapid development of this understanding across all socio-economic groups would facilitate growth adding to GDP.

IoT devices will create a lot data on individual consumers, through wearable devices, which type of music they like in various moods to their health vital stats leading to understanding of life expectancy. Driving habits through collection of data from car sensors is another set of data likely to have far reaching implications. Consumers must have a good understanding the potential benefits and risks on signing up to services that include IoT and Ofcom have a key role to help educate the consumer in order to facilitate safe IoT expansion.

9. Data analysis and exploitation:

10. International developments:

In terms of spectrum and operability, it is very important that devices can work in other countries. This is less so for sensors used in the house, however for any automotive M2M or various Smart City aspects, it is clear that they must have connectivity within continental Europe at least.

11. Ofcom's role :

Ofcom should be an enabler to support the growth of IoT in the right way to the benefit of both consumers and the wider economy

- Make the optimum spectrum available for IoT use to minimise interference and ensure adequate security is in place to protect it
- Ensure minimum standards and SLAs are in place and enforceable to guarantee continuity of the underlying infrastructure
- Consider measures to safeguard future IoT infrastructure as a part of the Critical National Infrastructure
- Support a standardised accreditation scheme for IoT devices, manufacturers and retailers around security and data privacy to add credibility
- Sponsor the education of consumers and other stakeholders around the merits, risks and safeguards of the IoT to facilitate adoption and growth

12. Additional comments: