Communications Consumer Panel and ACOD response to Ofcom's Call for input on promoting investment and innovation in the Internet of Things

The Communications Consumer Panel (the Panel) and the Advisory Committee on Older and Disabled People (ACOD) welcome this opportunity to respond to Ofcom's Call for input on promoting investment and innovation in the Internet of Things. The Panel works to protect and promote people's interests in the communications sector. We are an independent body set up under the Communications Act 2003. The Panel carries out research, provides advice and encourages Ofcom, government, the EU, industry and others to look at issues through the eyes of consumers, citizens and microbusinesses.

The Panel pays particular attention to the needs of older people and people with disabilities, the needs of people in rural areas and people on low incomes, and the needs of micro businesses, which have many of the same problems as individual consumers. Through its Members, the Panel represents the interests of consumers in Scotland, Wales, Northern Ireland and England. Following the alignment of ACOD with the Panel, the Panel is more alert than ever to the interests of older and disabled consumers and citizens.

Introduction

The Internet of Things (IoT) offers many exciting possibilities for UK consumers and citizens, but its development also leads to concerns in relation to privacy, data protection, the control of data and security. This is particularly relevant to the growth of big data – especially that of machine to machine data. What sets this apart from our current situation is the new development of aggregated data and inferred data. So while there are great opportunities for innovation, there are risks too. Consumers need to be given the tools to control their data and understand how data has evolved, how it will in future (e.g. the Proteus Pill), the value of their data and the implications of their consent to its release and use. Companies need to ensure that they have a compliance culture (which could involve a Code of Conduct for example) - to supplement any existing regulatory framework - and adhere to it.

Ultimately, there is a need for transparency, trust and fairness.

Inclusive Design

The Panel understands that the IoT potentially offers the possibility of providing a significant improvement in the lives of people with disabilities and may help to improve

quality of life. Connected devices offer people with disabilities, that prevent them from direct interaction with objects in their typical locations, the possibility of control via a mobile app. Connected devices also offer easier control to people who may struggle with a particular device, but can access and interact with it through tailored setups on their own mobile phones or other devices.

New applications may allow us to interact with technology in previously unimaginable ways e.g. the work on Lechal – a haptic feedback based navigation shoe that aims to assist blind and visually impaired people. As researchers Louis Coetzee and Guillaume Olivier at South Africa's Council for Scientific and Industrial Research (CSIR) noted in a 2012 research paper: "*The precise form and function of how IoT can break the accessibility barriers are not known yet. What is known is that inclusive design needs to be a fundamental element in the creation of IoT-enabled smart environments. Adopting a philosophy of creating an enabling environment through IoT, which embodies inclusiveness rather than just a smart environment, will go a long way towards ensuring inclusion in our technological futures.*"

Clear user interfaces are vital and we are conscious that some expert groups, e.g. euroblind, have put forward the case for a standardisation process defining the way to implement and use each of the IoT elements – although we are aware that the pursuit of such can sometimes lead to a slowing of progress. Euroblind argue that without a clear definition of standards, market and companies' commercial interests would lead each of them to apply their own technologies and definitions, resulting in a non-uniform set of access systems to information. They state that in the particular case of people with disabilities, this would mean their exclusion.

Privacy and data protection – trust and control

Currently, just over three-quarters of UK adults (77% - 1st quarter 2014[1]) have fixed or mobile broadband and consumers have access to a vast range of online services and applications. Many of these are free at the point of use, but these are often funded indirectly by the data that consumers provide about themselves and the websites they visit. The challenges that we currently face in relation to the privacy of data and data protection will become more sharply defined with the development of the IoT. However we now have an opportunity to learn from the experiences of the use of data online and how it has been utilised along the value chain by some commercial organisations, sometimes to detrimental effect for the consumer - e.g. as a partial cause of nuisance calls.

Sometimes online consumers knowingly provide personal data to third parties – but sometimes they do so without realising the possible consequences. Even where consumers know that they are supplying personal data, they generally do not realise that they are part of a lucrative and complex value chain that is part of an online information industry.

[1] Ofcom 2014 http://media.ofcom.org.uk/facts/

For consumers, providing personal data can have significant benefits in the form of services and applications that are more tailored to their needs, or that they might otherwise have to pay for. But there are also risks – that consumers disclose personal information without understanding how it is used or by whom, that data is misused, and that the law does not keep pace with industry developments or consumers' expectations.

Additionally, a lack of trust and understanding among users could become a barrier to the continued development of innovative services and applications, and the benefits for consumers that they bring.

Against this backdrop, in 2011 the Panel decided to carry out quantitative and qualitative research with consumers[2] to understand:

- how concerned people were about data gathering;
- the extent to which they were aware of the various methods of collecting data online;
- the extent to which consumers were prepared to share their own data and what they expected in return; and
- what steps, if any, they took to exercise control over the collection of their data.

The research, *Online Data: a Consumer Perspective*, found that there was a high level of awareness that companies collect customers' personal information (85%)- e.g. by asking people to register details with them, and through choosing to opt in or out of receiving marketing information, but there was less awareness of passive collection methods.

Only a small minority of respondents were always happy for the methods of data collection we asked about to be used for any reason. In general, younger age groups were more relaxed. Respondents were slightly more comfortable if their data was collected by a company/brand they trusted.

Levels of concern were also lower if the personal information was being used by companies to develop new business and services (31% had a high level of concern) than if it was being sold to third parties for them to target the consumer with products/services (79% had a high level of concern). Respondents said they were more comfortable about their data being used when they had control over whether this happened, and knew how the data would be used.

Respondents had relatively high levels of awareness of the types of methods that could be used to protect their information online but use of these methods varied significantly. Reactive methods were used much more – 73% of internet users said they regularly opted out of receiving marketing/information from companies and 50% of respondents said they regularly read companies' privacy statements to inform their judgements.

[2] http://www.communicationsconsumerpanel.org.uk/online-personal-data/online-personal-data-1
1,000 telephone interviews with a representative sample of UK internet users aged 16+. Ten in-depth telephone interviews, lasting approximately 30 minutes each.

While 12% of respondents felt that enough was currently being done to protect their information online, 22% were unaware of what was being done; 66% of internet users felt more should be done to protect their personal information on the internet.

The qualitative research echoed the range of views found in the quantitative study:

"I hate when you can't get to a certain page without opting in or registering. I don't like not knowing what they want my information for, especially if it is not a website that I am familiar with." (Male, 35-44 years old, Edinburgh)

"I don't mind so much if one company has a piece of information but it's when they start joining it together that I don't like it. Even if they ask for your permission it's the principle that bothers me." (Male, 35-44 years old, Birmingham)

"People should have responsibility for their own information. But I do think that things can be done to protect people's information more. The companies need to let the people know if their information is being used and how it is being used." (16-24 years old)

Similar themes emerge from a number of other more recent studies:

The European Commission's Special EuroBarometer 359 – Attitudes on Data Protection and Electronic Identity in the European Union (June 2011) - found that in relation to UK respondents:

- Trust: 54% of all those interviewed in the UK did not trust internet companies - e.g. search engines, social networking sites, e-mail services - to protect their personal data.
- Clarity of use: 80% were concerned that companies holding personal information may sometimes use it for a purpose other than that for which it was collected (e.g. for direct marketing or targeted online advertising), without informing the individuals concerned.
- Consent: 94% of those interviewed agreed that specific approval should be required to collect and process personal information and that if this information had been lost or stolen that they would want to be informed.

O2 Telefónica's survey "The Data Dialogue" of over 5,000 citizens examined the public's attitudes toward privacy and information sharing and found that:

- There is no single attitude to sharing personal information.
- The public is aware that personal information and behavioural data are used for commercial purposes, although understanding about what this means in practice is limited.
- People are sharing more than ever, but there is a 'crisis of confidence' in the way that personal information and behaviour data are being used.
- Losing control of personal information is a significant concern.
- The public will welcome measures to give them more control over personal information and behavioural data, especially knowing what is held about them, and the ability to withdraw it if they wish.

And finally, in 2013, Microsoft & IIC's global research[3] "Personal data management: the user's perspective" found that while many participants accept a level of both personal accountability and responsibility for what they put online, they express a desire to exercise control over what happens to their personal data and how it is used.

From the research the Panel concluded:

- People are generating large volumes of data without realising it through their online engagement.
- There is a lack of transparency around who is doing what with people's data. This could impact people's trust in online engagement.
- People feel they are losing control of their personal data.

Gaining consumers' trust has always been important, but in the online world it is becoming increasingly so, as more government services are going 'digital by default'. Ensuring trust will also enable people to engage more comfortably with new and innovative services.

We are also concerned that there may be a risk that switching may be made more difficult in some contexts eg if smart meters from each provider didn't have some degree of interoperability. Smart devices could potentially become a way of potentially capturing customers and making switching costly/impossible.

The IoT will potentially involve a vast increase in the collection and transmittal of data – and particularly sensitive personal data. The protection of this data is paramount. Automated decision making and inferred data are areas of particular concern – how would a consumer know if an error has been made in a calculation on which decisions are based – and equally importantly, how would they report any security breaches and get incorrect information corrected and gain redress?

Consumers can only take responsibility if they know how their data is being collected and processed and have the tools to manage its use. This should not mean making privacy policies longer and more complicated – in fact there is a case for simplifying such information. Consumers should also be able to reverse decisions that they have made to share personal data. Companies need to use their expertise in content presentation to provide privacy information and tools in user-friendly ways, for example by providing terms and conditions that do not run to tens of pages of legal terminology that is inaccessible to the majority of consumers.

We believe that consumer-centric policies are needed - clear and layered privacy notices and flexible regulations that allow innovation but hold companies responsible if they misuse data. It is also pertinent to start to consider who should act as the data controller and the potential role of third parties and tools such as privacy seals. Essentially privacy should be enshrined by excellent design.

[3] Research carried out in Canada, China, Germany and US

With evolving technology enabling creation and capture of greater amounts of data, the Panel believe more could collectively be done to:

1. Provide “easy to understand” information to allow people to make an informed decision about the implications of releasing their data;
2. Raise people’s awareness of what data is being collected, how it is collected, what is being done with it, by whom (which third party) and for how long the data will be held and used;
3. Enable the individual to have more control over their own personal data;
4. Provide reassurance that companies will always minimise the amount of data that they collect, store it securely, retain it for no longer than is necessary – and consider whether to check with consumers after a set period of time whether they still wish their data to be retained; and,
5. Give people confidence that companies will follow the rules and manage personal data responsibly - and that if they do not, they will face robust enforcement action.

Security

We are conscious of the need for robust security processes. In addition to the potential capture of sensitive data, there is the risk that IoT devices could be hacked in ways unbeknown to the user. We have already seen examples of this – and it is of particular concern that some devices lack the capability of being adjusted by the consumer to change or increase security levels – e.g. password setting. The systems must be able to authenticate transmissions at the level of both device and user. If wider connectivity between "things" isn't collectively and individually secure, then all it might require is for one weak point for unauthorised users to gain access.

Network security and reliability of supply take on added importance in the context of the IoT. If, for example, wellbeing and healthcare are managed via the IoT, the quality and consistency of supply is paramount. If issues should occur, there needs to be fast and effective back up and a safety net of some kind - especially for the more vulnerable. We would also welcome further information about whether the co-allocation of relevant spectrum could raise security concerns.

Exploiting the benefits for consumers must surely start with full awareness and understanding, and then true benefits must be identified and appropriately regulated. Although industry may be best placed to lead development in many respects, we would like to see Ofcom take a proactive role when it comes to assessing consumer impacts, protection and awareness.

Summary

- The IoT offers exciting possibilities for UK consumers and citizens, but its development also leads to concerns in relation to privacy, data protection, the control of data and security.

- Consumers need to be given the tools to control their data and understand how data has evolved, how it will in future, the value of their data and the implications of their consent to its release and use.
- Companies need to ensure that they have a compliance culture and adhere to it.
- Ultimately, there is a need for transparency, trust and fairness.
- The IoT potentially offers the possibility of providing a significant improvement in the lives of people with disabilities and may help to improve quality of life.
- Clear user interfaces are vital - we are conscious that some expert groups have put forward the case for a standardisation process although we are aware that the pursuit of such can sometimes lead to a slowing of progress.
- The challenges that we currently face in relation to the privacy of data and data protection will become more sharply defined with the development of the IoT. However we now have an opportunity to learn from the experiences of the use of data online and how it has been utilised along the value chain by some commercial organisations, sometimes to detrimental effect for the consumer.
- The IoT will potentially involve a vast increase in the collection and transmittal of data – and particularly sensitive personal data. The protection of this data is paramount. Automated decision making and inferred data are areas of particular concern.
- We are conscious of the need for robust security processes. In addition to the potential capture of sensitive data, there is the risk that IoT devices could be hacked in ways unbeknown to the user.
- Network security and reliability of supply take on added importance in the context of the IoT. If issues should occur, there needs to be fast and effective backup and a safety net of some kind - especially for the more vulnerable.
- Although industry may be best placed to lead development in many respects, we would like to see Ofcom take a proactive role when it comes to assessing consumer impacts, protection and awareness.