Enabling the
information society

BCS, The Chartered Institute for IT
Consultation Response to:

Ofcom Promoting investment and innovation in the Internet of Things
Dated: 1 October 2014

BCS
The Chartered Institute for IT
First Floor, Block D
North Star House
North Star Avenue
Swindon SN2 1FA

BCS, The Chartered Institute for IT

The Institute promotes wider social and economic progress through the advancement of information technology science and practice. We bring together industry, academics, practitioners and government to share knowledge, promote new thinking, inform the design of new curricula, shape public policy and inform the public.

As the professional membership and accreditation body for IT, we serve over 70,000 members including practitioners, businesses, academics and students, in the UK and internationally. We deliver a range of professional development tools for practitioners and employees.

A leading IT qualification body, we offer a range of widely recognised professional and end-user qualifications.

www.bcs.org

Ofcom Promoting investment and innovation in the Internet of Things Dated: 1 October 2014

Consultation Document:
http://stakeholders.ofcom.org.uk/binaries/consultations/iot/summary/iot-cfi.pdf

Summary of BCS calls for action:

- Changes in the short range wireless community should be overseen by Ofcom and ensure that backwards capability becomes mandated;
- Best practice guidance from Ofcom would help ensure that potential system compromises would be avoided;
- The development of safe software practices should be enforced;
- Regulation is needed for some of the newer technologies;
- It is essential that organisations conduct security reviews of their products;
- API management systems should be implemented to ensure that data is not interrupted between devices;
- Regulatory enforcement will be fundamental to the consumer trust of IoT;
- Ofcom should be proactive in encouraging and facilitating methods of obtaining and recording informed consent;
- Ofcom could provide easy to understand examples of concise agreements, encourage the development of authentication and consent technology;
- Ofcom should work ODI and similar groups around the world to help develop reliable data resources to underpin IoT;
- It is important that Ofcom work in partnership with regulators, standards bodies, research bodies and the ITU;
- Industry is best placed to focus the development, standardisation and commercialisation of new technology and exploit its full potential.

1.46 IoT definition, applications and demand

BCS defines the IoT as; *Interconnected objects which contain embedded technology (e.g. sensors) to communicate, sense and interact electronically with the environment in which they are placed. As more information is produced these objects will interact between themselves with the aim to improve the quality of human life.*

Such technologies have been around for decades in ‘vertical’ markets, such as M2M, telematics, and Building Management Systems. The advent of cheap processors and sensor devices together with low power wireless communications allowed rapid development of IoT. Big Data analytics and cloud computing mean that the boundaries between vertical markets cease to exist. Benefits to consumers and businesses increase as the boundaries between business and consumers/employees merge.

Operational efficiency of buildings and systems sensitive to the presence, role and activities of the humans inside are now producing amazing savings in energy, more efficient business processes and happier employees. Sensitive regulation should still protect the consumer but not over restrict the business and reduce innovative investment.

In Ofcom’s traditional role, it has influence in the sectors related to telecommunications and broadcasting. IoT will take it into all areas of business and private life where ‘connected devices’ are used.

1.47 Spectrum requirements

Most IoT projects use technology with very low data rates. Wide coverage, availability and power efficiency is more important than bandwidth. This is a generalisation but as Ofcom knows, spectrum is not finite and therefore it is likely that two or three different scenarios will be needed to deal with demand in spectrum space and differentiate business and consumer issues.

Characteristics of devices and applications are likely change very fast and therefore it could be wasted effort trying to profile applications. What will be required for innovation is an affordable cost model for spectrum for entrepreneurs and developers. Many IoT devices are using ‘white space’ or unlicensed spectrum for connectivity. The majority of applications and services will however be delivered through internet interfaces.

It has been assumed that sensors and IoT devices will have predictable spectrum needs related to normal market growth trends. There are occasions when the unpredictable happens such as SMS demand in 2G or the personal media content on mobile phones. Nobody could have predicted the ‘selfie’ but the bandwidth demand from user generated content is significant. Similarly, the IoT equivalent could well disrupt spectrum planning. Ofcom should do everything in its power to stay ahead of the game in monitoring and predicting anomalies in network growth.

1.48 Network-related issues

SMS was originally developed as an M2M technology for network engineers and currently Global System for Mobile Communications (GSM) is the most widely owned technology in the world. Its bandwidth is more than adequate for most IoT applications, and the 800 – 900MHz bands where it operates in UK give good coverage and building penetration.

The integration of multiple devices in a small local deployment, for example in a home, might require a shared spectrum model. Broadcast entertainment requires high bandwidth but smart meters and security systems do not. BCS therefore predicts that as the number of these devices increase so will the pressure placed on bandwidth and service differentiation. The low demand services e.g. white goods, heating, garage doors etc. could be clustered on a low bandwidth service while broadcast media, gaming and maybe CCTV security could be clustered on Wi-Fi and fast broadband.

The business case for mobile network growth depends on the number of users paying for services and bandwidth. The extremely high numbers of connected devices anticipated for IoT, mostly long life sensors with very low data rates, will place demands on the switching infrastructure which is not charged for currently. A single sensor might poll the network 9 or 10 times to send 100 bytes but a closely arranged set could stress the network switching making IoT an expensive service to deploy with little monetisation from bandwidth. Alternative local hub technologies to deal with this are available and should be covered by regulation especially for privacy, safety and security issues.

The UK's business broadband is regarded by BCS as inadequate and we are working with other organisations (such as the DPA, INCA, FSB) to feed back our views to Government (including the current DCMS consultation). In the IoT context, this is primarily a lack of fibre backhaul to the wireless services.

Changes in the short range wireless community should be overseen by Ofcom in the interests of the market. Re-purposing of 2G infrastructure is becoming an issue and if it is done in a way to support IoT development then Ofcom should encourage it. One example might be the LTE-M pilot from Vodafone. Planning for 5G is anticipating a multi- technology infrastructure with multiple new radio networks. It is vital that Ofcom mandate backwards compatibility as these new services develop.

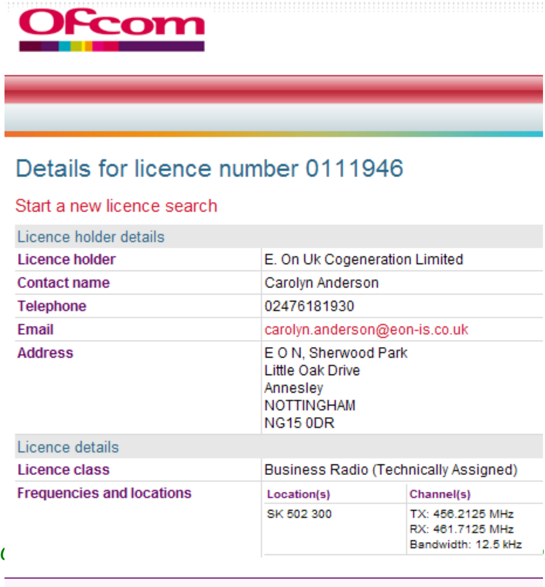
1.49 Security and resilience

Used correctly IoT will enhance the detection of and recovery from security incidents. Layer 7 Technologies will shortly be able to automate dynamic recovery of IoT services.

At a recent Cambridge wireless CNI meeting, several of the speakers mentioned that generic network devices designed for service delivery and management come pre-infected with StuxNet Virus. Regulatory attention to this with mandatory pre-delivery testing is critical.

Much of the early life of IoT systems is supported on generic development boards such as Arduino or Raspberry Pi. These typically have unused ports which could be used to compromise the system. Best practice guidance from Ofcom would help in removing this threat. We feel that development of safe software practises should be enforced. Standards for this exist and are used widely in the CNI resources.

One major anomaly, which Ofcom is responsible for, is the insistence that wireless frequencies, licensee details etc. are published openly, as per the examples below. This gives a catalogue for potential terrorists and criminals to pick from.

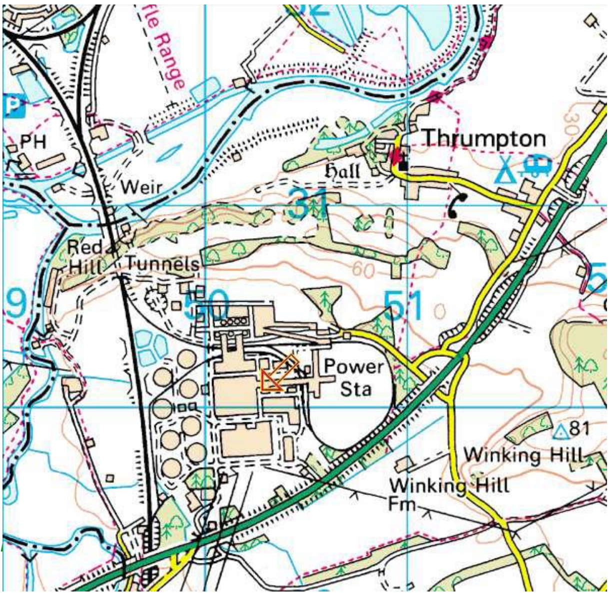


Ofcom

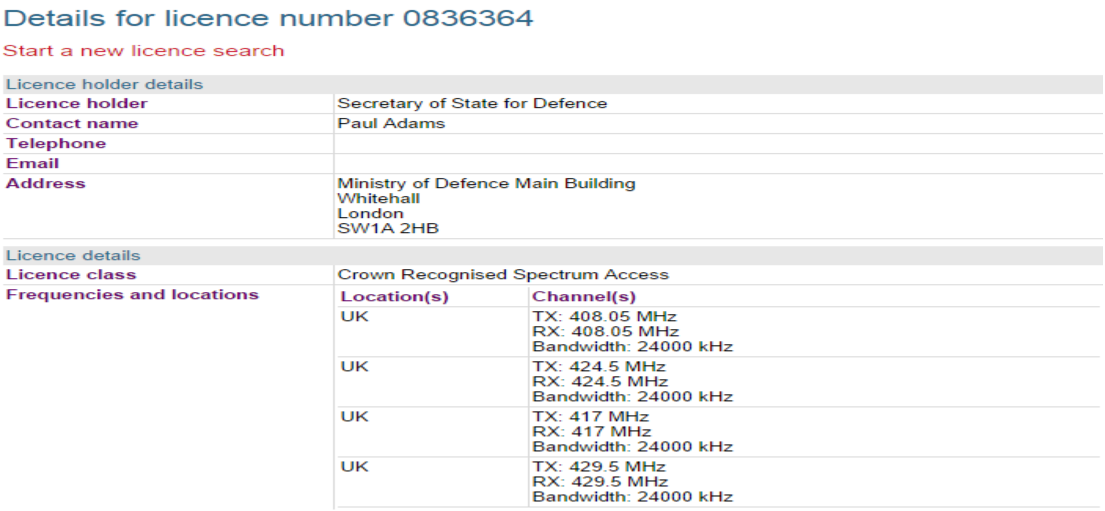
Details for licence number 0111946

Start a new licence search

Licence holder details	
Licence holder	E. On Uk Cogeneration Limited
Contact name	Carolyn Anderson
Telephone	02476181930
Email	carolyn.anderson@eon-is.co.uk
Address	E O N, Sherwood Park Little Oak Drive Annesley NOTTINGHAM NG15 0DR
Licence details	
Licence class	Business Radio (Technically Assigned)
Frequencies and locations	Location(s): SK 502 300 Channel(s): TX: 456.2125 MHz RX: 461.7125 MHz Bandwidth: 12.5 kHz



Co *nt a*



Details for licence number 0836364

Start a new licence search

Licence holder details		
Licence holder	Secretary of State for Defence	
Contact name	Paul Adams	
Telephone		
Email		
Address	Ministry of Defence Main Building Whitehall London SW1A 2HB	
Licence details		
Licence class	Crown Recognised Spectrum Access	
Frequencies and locations	Location(s)	Channel(s)
	UK	TX: 408.05 MHz RX: 408.05 MHz Bandwidth: 24000 kHz
	UK	TX: 424.5 MHz RX: 424.5 MHz Bandwidth: 24000 kHz
	UK	TX: 417 MHz RX: 417 MHz Bandwidth: 24000 kHz
	UK	TX: 429.5 MHz RX: 429.5 MHz Bandwidth: 24000 kHz

Regulation is needed for some of the newer wireless technologies, such as BLE Beacons in retail, home and business environments. DLNA, present in most modern domestic devices, are totally open and insecure. This needs to be addressed with some urgency.

BCS believes that it essential that organisations conduct security reviews of their products, including the devices themselves, controlling apps and ensure that their communications protocols are in place. Additionally, businesses need to monitor the life cycle of data from when a customer supplies you with their details, or accesses a device, to when they leave. It could also be argued that the IoT needs its own security model in order to fully protect user data, allowing the data to be shared in a secure manner. We would encourage those operating IoT to implement stringent API management systems (API portals and gateways) and ensure that data is not interrupted between devices.

1.50 Data privacy

Most homes will be ‘multi-hub’ with separate facilities for differing services, e.g. the home entertainment hub, the ‘white goods’ hub, the ‘energy/smart meter’ hub, the ‘security’ hub etc. All these will provide data which is currently the property of the householder(s). Regulation must ensure that this remains so. ‘Invisible’ tracking through DLNA and possibly Bluetooth or WiFi correlated with data from the mobile phones in the room can generate huge volumes of personal data.

Remote access and use of this data by persons other than the householder must, even under current legislation, be with specific informed consent. Unfortunately, there are already devices in most homes which do not comply with this basic privacy rule and the resulting personal information is being marketed without the knowledge or consent of the owner. An example of this is the monitoring of the TV channel being watched, probably recorded in conjunction with the identity of the watcher. This information will most probably be derived from identification of the watcher’s mobile phone. This information is sold back to TV advertisers so that advertising is delivered according to the tastes of the watcher. Regulatory enforcement of existing regulations and support of forthcoming ones will be fundamental to the consumer trust of IoT (and therefore its adoption and growth).

Correlation and advanced analytic techniques can add new dimensions to the invasion of privacy and other possible criminal activity. The data acquired by one utility should be used only for the purpose for which it was collected and not be passed on or traded without the specific permission of the consumer. There is no such thing as anonymised data as two unique identifiers from one context can be used to break anonymisation in another.

Ofcom should be proactive in encouraging and facilitating methods of obtaining and recording informed consent. Cookie law is an acknowledged failure and ever longer privacy agreements on products give no protection to the consumer. There are many signs that the privacy backlash is here. A survey from TRUSTe showed that of the 54% of consumers who were aware of privacy issues on the internet 90% said they were concerned about privacy. It is not necessarily an age related issue as 14 and 15 year old UK students conducted international surveys on privacy last year. They presented their results at the Internet Governance Forum in Bali as evidence that their generation was fed up with being tracked. Ofcom could provide easy to understand examples of concise agreements and encourage the development of authentication and consent technology such as UNI-IDM from Royal Holloway University. It is imperative that companies are honest and up front with consumers about the type of data that is being collected about consumers and how they can control its potential uses. Companies need to look at improving the security arrangements around the collection and transmission of data to protect against hacking and to provide secure authentication of senders and recipients of data.

Unregulated deployment of low power (BLE) Bluetooth beacons mentioned in the previous answer could cause much invasion of privacy. Current Bluetooth4 low power chips have a range approaching half a mile.

BCS agrees with the ARM and AMD report that more needs to be done to reassure consumers about the security arrangements for (i) protecting their data against hacking and (ii) ensuring their data is not transferred to an unauthorised recipient[1]. Consumers should be informed of the benefits gained from agreeing to their data being used. There should be debate about this, which ensures that consumer confidence is maintained without stifling the opportunity for innovation. The debate should be framed around some key principles, such as the need to provide consumers with a clear and succinct method of understanding how their data will be used (and the possibility to opt out).

In a survey conducted by BCS, 94 per cent of respondents thought there should be tighter regulation on the use of personal data. 74 per cent felt the same about comparable regulation on business.

We believe that the Information Commissioner should remain the independent regulatory office dealing with data protection and privacy issues in the UK.

[1] http://media.corporate-ir.net/media_files/IROL/19/197211/ARM%20and%20AMD%20-%20Data%20Management%20in%20the%20Internet%20of%20Things.pdf

1.51 Numbering and addressing

Registration of numbers and addresses falls under current regulatory controls, such as the Regulation of Investigatory Powers Act. There are potential privacy and security risks from the monitoring or misuse of device addresses, especially when they can be paired with people or businesses. Identification of these devices other than for the operational deployment and management of IoT services will need to be controlled.

Vulnerability of devices to cyber threats and malware will result if dumb devices can be ‘spoofed’ because their details are available to criminals. Self deploying and provisioning networks are becoming available as software defined networks. These have the ability to self audit the transactions between ‘things’. Protocols are also being developed by some stakeholders e.g. ARM, for the IoT devices to ‘advertise’ their capabilities so that applications requiring their information can collect it. These could present a regulatory challenge and be almost impossible to monitor. BCS sees no need for significant changes in the provision of telephone numbers and with IPV6 the number of IP addresses is adequate.

1.52 Devices

One of the main issues associated with IoT is the lack of interoperability between devices belonging to different systems. There is a battle between proprietary platforms, which allow the interoperability only of devices that have been certified by the manufacturer of the IoT system and open source platforms[2]. BCS believes that there is a clear need for a common language of communication through an “architectural reference model for the interoperability of IoT systems”[3]. Open source platforms allow any possible device to connect to their systems and help allow devices to connect seamlessly and remain free from closed, proprietary standards[4].
We agree with the Silicon Labs report that “there is no one wireless or wireline technology that can efficiently serve across an entire network”. To develop cost-effective products, engineers will need to be able to select the optimal communications channel and protocol for their application[5]. It is assumed that IoT is likely to be based on a variety of standard and proprietary protocols.

Recent research conducted by HP revealed that the average IoT device has 25 security flaws and as the number of connected IoT devices constantly increases, security concerns are also exponentially multiplied. BCS believes that coupled with privacy, concerns about security of data could restrict the IoT. Greater emphasis needs to be placed on incorporating security into IoT devices at the design point. The Canadian privacy by design policy is gaining worldwide popularity. Similarly, security chips like TPM Modules commonly fitted to secure laptops are finding their way into other markets. If very high security is needed this could be mandated.

[2] http://blogs.dlapiper.com/iptitaly/internet-of-things-proprietary-vs-open-source-systems/

[3] http://blogs.dlapiper.com/iptitaly/internet-of-things-proprietary-vs-open-source-systems/

[4] http://www.lexology.com/library/detail.aspx?g=a1d7ef89-58e8-4c87-99d1-d4fb94f2a3d2

[5] http://www.silabs.com/Support%20Documents/TechnicalDocs/bringing-the-internet-of-things-to-life.pdf

1.53 Digital literacy

Some studies need to be done to understand the needs of the wider community particularly in specific market sectors where specialist terminology or practises exist, for example, medical informatics or smart cities.

BCS would be happy to work with Ofcom in developing and delivering suitable materials to address any needs found.

1.54 Data analysis and exploitation

Following from our comments on data privacy above, we endorse the open data movement and in particular the ODI in registering and licensing data sets. We have seen developments in analysis and 3D Visualisation of this data such as the real time London underground and bus models shown by Vizicities.

Big Data applications delivered alongside other similar models (in a lightly regulated environment) will transform our understanding and interaction with the IoT and our world.

Ofcom should work with ODI and similar groups around the world to help develop reliable data resources to underpin IoT.

1.55 International developments

BCS strongly believes that the success of the IoT is dependent on the operation of global standards. It is therefore important that Ofcom work in partnership with regulators, standards bodies, research organisations and the ITU.

Presentations given at the recent 5GHuddle event in London highlighted the impact of IoT on the development of 5G infrastructure. Presentations given from all over the world showed that for once all these global stakeholders are working together and in this instance IoT is on the agenda as a fundamental service. Of significance, were consolidated views from regulatory groups in China, Korea, Japan, India, Europe and North America. It is anticipated that in supporting IoT devices (with high density and low bandwidth) as well as very high bandwidth services, the developing infrastructure will need to support everything from current to 20GHz+ mmWave frequency bands. These will be non-cellular cognitive radio networks with low latency SDN self organising networks. Flexible and virtual Radio Access Networks (RANs) with massive MIMO or other antennas will ensure coverage.

The UK Government has done well in establishing the 5GIC at Surrey University as a world standard institution with major UK Stakeholders. Rahim Tefazolli, its Principal, has said that the main challenges are latencies, reliability, security/privacy and energy efficiency[6].

[6] https://eu-ems.com/event_images/presentations/Rahim%20Tafazolli%20-%20Part%201.pdf

1.56 Ofcom's role

BCS believes that Ofcom will play an important role in regulating and enabling a network of wireless devices.

In the context of developing investment and innovation:

Traditional M2M, telematics and industrial automation have stayed relatively isolated 'vertical' applications. As they share their capabilities and new services are developed with B2C and B2B market aspirations much will come from totally new business models. Big Data analytics will underpin this as the ability to show previously unrelated events can be analysed in ways that allow new predictions. New services built on these predictions might offer regulatory challenges which will require great flexibility and innovation in Ofcom itself if these markets are to grow. New challenges about the ownership of data derived from 'things' might well stretch Ofcom's flexibility even more.

Unfortunately, the B2C market will be plagued with misuse of the consumer data in targeted 'advertising pays' business propositions as described above. This will need to be addressed. Alternative investment in infrastructure and services is becoming critical, particularly the provision of widespread backhaul for wireless services. A privacy backlash as mentioned before could weaken investment based on advertising.

The open data collaborative commons phenomenon is stimulating more free services. This again will be a challenge for regulation of fair competition by Ofcom and undermine investment.

As devices become more part of human life then users will become more dependent on them. As direct device interaction develops through perhaps eye tracking, voice interaction, bio sensing and motion monitoring a human dependency will grow. These devices will feed back or react to human feelings, health or similar personal indicators and become trusted assistants. Services such as healthcare, finance, entertainment and education will all be personalised to an extent when people will be lost without the devices. Regulatory engagement and enforcement will need great sensitivity in this world of things.

Smart city investment derived from the communities served is spawning new models. In addition to securing the social inclusion budget some cities are encouraging investments from local businesses working with local telecommunications and infrastructure providers. Malmo has a system where investment in energy efficient 'smart' infrastructure has turned the failing local economy round. Projects for heat extraction, waste 'Grey Water,' energy efficient housing, smart meters and smart grids were funded by innovative 'Development Bonds' raised from local businesses. The improved quality of life is now making these investment bonds show a profit to the local community. Similar financial and investment innovation could be encouraged by Ofcom to stimulate growth.

Additional comments

Fundamental to the success of IoT in building new services and improving efficiencies is the marriage of diverse communications and sensing infrastructure with Big Data analytics. This means that not only can we collect vast amounts of data from connected devices and sensors, we can analyse this data in new ways giving rise to totally different and often unexpected results.
We agree that industry is best placed to focus the development, standardisation and commercialisation of new technology and exploit its full potential. Industry, academia and professional bodies should thus drive the development of standards for IoT- optimised variants of

existing technologies. That said, consumerisation and unregulated provisioning of IT is particularly active in the IoT area so Ofcom's consumer protection brief, if sensitively applied, could be very beneficial. However, this should not stifle innovation and growth.

At the recent IoT event at the Science Museum in London both Ed Vaizey MP and the Chairman of ARM stressed that specific ownership and control of all personal data derived from the IoT by the individual was fundamental. The recent Ofcom communication giving guidance on the safe use of mobile phones was a good example of the promotional and supportive role of Ofcom.

We would welcome further dialogue with Ofcom in regards to strategies to ensure that the UK is able to take advantage of the opportunities for growth and innovation associated with the IoT.

End