Comments of Cisco Systems

Ofcom consultation on 'Promoting investment and innovation in the Internet of Things'

Submitted 1st October 2014

Introduction

Cisco welcomes the opportunity to respond to the Ofcom consultation on 'Promoting investment and innovation in the Internet of Things' published on 23rd July 2014.[1] We believe the UK is taking an important lead in driving this topic and are particularly pleased that Ofcom is approaching the topic by recognising the opportunities that the Internet of Things (IoT) is and will bring, not just the potential challenges. According to a Cisco study[2], over the next decade (2013 – 2022) there is $14.4 trillion value at stake globally for the private sector and $4.6 trillion for the public sector.

Ofcom is no doubt well aware that it is not acting in isolation in this space and given many of the topics to be addressed are a joint remit with UK government departments and agencies we urge Ofcom to work in a coordinated fashion with their colleagues. Likewise, discussions on IoT are emerging across Europe and globally, and we encourage Ofcom to engage and lead discussions with their colleagues in the ITU, RSPG/RSC, CEPT, BEREC and with the European Commission, as well as with other international partners.

We believe that Ofcom has successfully identified many of the relevant topics in the policy environment, and we look to answer to each of the identified sections below. These include an overview of IoT applications and demand; devices,

[1] http://stakeholders.ofcom.org.uk/consultations/iot/intro
[2] IoE Value at Stake, Cisco, 2013 http://internetofeverything.cisco.com

technological trends and commercial deployment; network-related issues; standards and interoperability; spectrum requirements; security; data privacy; numbering and addressing; digital literacy and big data. In addition, we highlight the need to make a coordinated assessment of legal frameworks in regulated sectors.

1. IoT definition, applications and demand

Cisco distinguishes the Internet of Things from the Internet of Everything (IoE), which is the networked connection of people, process, data and things. It encompasses machine-to-machine (M2M), machine-to-person (M2P) and person-to-person (P2P) connections. It is about connecting people in more relevant ways; enabling the right information to reach the right person or machine at the right time; converting data into usable intelligence; and connecting devices to the internet and each other. By contrast, the IoT does not account for the people and process elements of the IoE.

Ofcom characterizes the IoT as M2M connections and interconnection between multiple M2M applications. While this is interesting in itself, Cisco believes a more holistic approach better underscores how the internet and IP networks are developing and how they are shaping our society.

To avoid confusion and to answer the specific enquiries of Ofcom, however, after an initial discussion on the differences in definition and impact on demand in this section we will revert to using IoT or M2M for the rest of our response. In this specific section we will look to clearly distinguish when we are talking about M2M connections, whereas IoE will be used to denote when we are addressing M2M, M2P and P2P connections.

To further clarify the distinction between IoT and IoE, M2M applications account for 45% of the value at stake for the private sector, whereas M2P and P2P account for the other 55%. This is a more marked difference when it comes to

the public sector where 69% of the value stems from P2P, such as telework or connected learning, and M2P, such as video surveillance and smart parking.[3]

As the Ofcom consultation paper notes, accurate growth estimates for the number of connected objects can be difficult to establish and there is a range among estimates. The Cisco Visual Networking Index Global IP Traffic Forecast 2013 – 2018 predicts almost 21 billion networked devices by 2018, up from 12 billion in 2013.[4] Of these, 7.3 billion will be M2M modules, against 2.3 billion last year. The Global Information Technology Report 'Emerging Issues for our Hyperconnected World' put the range as between 20 billion and 50 billion by 2020 in various studies.[5] In the UK, the Aegis and Machina Research paper quoted in the consultation put the number of M2M connections at 370 million by 2022[6], whereas the Cisco VNI data pointed to 210 million M2M connections in the UK in 2018.[7], representing 43% of all connected devices. This figure is within the same order of magnitude as the Aegis and Machina prediction given the four-year difference, though it would require the predicted growth rate in the VNI to slow in order for the two predictions to match one another. M2M is expected to swiftly increase its share of total devices, increasing from 21%, or 60 million, in 2013, to 43% in 2018. This represents a 29% compound annual growth rate (CAGR).

Outside of these predictions, a good way of looking at the potential demand is that only 0.6% of all the objects that may one day be connected are connected today[8]. This is a huge opportunity for our economy and society.

The Ofcom consultation names examples from the healthcare, transport and energy sectors and asks for comment on which sectors stand to benefit from IoT.

---

[3] *Ibid.*

[4] Visual Networking Index Global IP Traffic Forecast 2013 – 2018, Cisco, 2014 http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.pdf

[5] Emerging Issues for our Hyperconnected World, Global Information Technology Report 2012, P. Biggs, T. Johnson, Y. Lozanova and N. Sundberg.

[6] M2M Application Characteristics and their Implications for Spectrum, Aegis and Machina Research for Ofcom, 2014 http://stakeholders.ofcom.org.uk/binaries/research/technology-research/2014/M2M_FinalReportApril2014.pdf i

[7] For UK-specific VNI data, please see the VNI Forecast Highlights Tool: http://www.cisco.com/web/solutions/sp/vni/vni_forecast_highlights/index.html

[8] IoE Value at Stake, *op. cit.*

A Cisco report from earlier this year, looking at the IoE in the UK, points to five verticals where the IoE can have the greatest impact in the shortest amount of time.[9] This mirrors healthcare, transport and energy as identified by Ofcom, and also includes retail and manufacturing. Healthcare applications, for example, include managing health conditions in real time without the need for entering an NHS practice or hospital. In a trial for the Airedale NHS Trust in West Yorkshire, over 1000 patients in 33 residential care homes were linked to medical professionals via secure video in a 24 hour Telemedicine Hub. The residents were also able to conduct face-to-face consultations with their caregivers over mobile video. The result was a 60% drop in the total number of hospital bed days, set against an 18% rise in days for car homes not using telemedicine in the same period.

Examining the private sector opportunity at the global level, the Cisco Value at Stake analysis puts figures on the industries that have the most to gain. The top four industry sectors were manufacturing, with 27% of the total value at stake, retail at 11% and information services and finance/ insurance at 9% each.[10] As this analysis is only for the private sector it is not surprising that healthcare and transport, both likely to be only partially in the private sector, are not in the top four. Nevertheless, it is striking how strong the opportunity in manufacturing is. The factors that create this value differ according to the use case. In manufacturing, it includes agility and flexibility in factories and making the most of workers' skills. In retail, on the other hand, connected marketing and advertising present the most value.

It is clear that the IoE, and within in the IoT, are expanding rapidly as we enter a new era for networking. Despite this ongoing success, and to a certain extent because of it, policymakers and regulators in the UK, Europe and across the globe need to get the policy environment right and maximize the economic and social benefits.

[9] The Internet of Everything: Bringing the future to life, Cisco, 2014 http://www.cisco.com/web/offer/grs/176780/The_Internet_of_Everything_Bringing_the_future_to_life_FINAL.PDF

[10] IoE Value at Stake *op. cit.*

2. Devices, technological trends and commercial developments

In a change from the order of the sections in the consultation, we have chosen to respond to the request for comment on devices early in our response as we believe that it helps set the scene for the sections below by shedding light on the reasons for the ongoing success of the IoT. We also take the opportunity to explain further technological and commercial drivers for the growth of the IoT.

Form factors continue to shrink, enabling smaller, cheaper and more intelligent devices and allowing for a wider and wider range of things to be connected. A computer the size of a grain of salt can now have a solar cell, a thin-film battery, memory, a pressure sensor and a wireless radio and antenna. A sensor the size of a speck of dust can detect and communicate temperature, pressure and movement. As the market continues to grow and as technology develops, Cisco expects factors to continue to shrink and the cost of production to decrease with economies of scale.

In terms of technological trends, we continue to see dramatic increases in storage, processing power and bandwidth at lower cost, even now in line with Moore's Law. Cloud and mobile computing facilitate the IoT, and hence their rapid expansion has a mutually beneficial impact. Given the vast amount of information produced by connected objects, 'big data' and our ability to analyse and make use of it is fundamentally tied to the success of the IoT and vice versa. Moreover, the IoT is benefitting from the improved ability to combine hardware and software.

Finally, business value creation has shifted to the ability to create intelligence from connections, and the IoT reflects this. Companies need to capture intelligence faster from sources outside themselves. Metcalfe's Law ensures that as the number of networked objects increases the number of connections grow at a faster rate.

3. Network-related issues

While M2M will make up 47% of connected devices in Western Europe by 2018, the proportion of total traffic it accounts for is much less, at 3.4%.[11] This is because an average M2M module created 78MB per month of traffic last year versus a typical PC creating 22.7GB. Proportionally, however, its growth is phenomenal. While the average PC traffic will almost double to 39.2GB per month in 2018, the average M2M module will create almost 7 times the amount of traffic by 2018 at 514MB. Coupled with the expansion in number of devices, and the traffic will be 22 times greater in 2018 than 2013 in Western Europe. Hence while the PC is declining from 67.2% to 42.8% of total traffic, M2M is increasing from 0.4% to 3.4%.

Interestingly, the average traffic from mobile M2M modules is only a little less than the overall average (including fixed modules).[12] It will increase by just over 7 times from 2013 to 2018, from 61MB per month to 451MB. Its overall growth is even more spectacular than for M2M modules overall, expanding by 43 times from 2013 to 2018 and reaching 5.7% of total mobile traffic.

Need for greater network bandwidth

The expansion in traffic dictates the need for greater network bandwidth for M2M. To meet this demand policy makers need to create the right policy framework to stimulate investment in more robust and higher speed broadband networks, both fixed and mobile. Platform competition is key (fixed, mobile and cable), while Next Generation Access Networks need to be fostered. All technologies have a role to play, but clearly FTTH is the end game in the wireline world – and it is important to support this transition. This requires new financing models and a greater use of public-private partnerships.

[11] VNI Global IP Traffic Update 2013 – 2018 *op. cit.*
[12] Visual Networking Index: Global Mobile Data Traffic Forecast Update 2013 – 2018, Cisco, 2014 http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.pdf

Need for appropriate and reasonable traffic management

But the IoE, and the IoT within it, require more than just more bandwidth. They will also require the ability to handle different feature requirements of traffic flows, from low latency for bidirectional high definition video to coping with data bursts for wireless data transfer. Intelligence will need to be built into both the edge of the network and in the data centre.

It will be essential to get net neutrality right and to enable appropriate traffic management and new business models. There will be an increased need for network resource management tools to handle the connected devices, their feature requirements and the data they produce. There is a need to make sure we can have reasonable and appropriate traffic management in the internet as well as allowing room for further innovation through managed or 'specialized services' along side the best effort internet.

This is being addressed on a pan-European basis in the draft Telecom Single Market Regulation.[13] The current draft net neutrality rules as amended by the European Parliament do not get this balance right in our view. Ofcom's role in this end sits within the wider context of the UK government and negotiations between Member States and in the European Parliament. Nevertheless, we urge the relevant parties in the UK to work with their peers to advocate for a balanced text that prevents bad behaviour (blocking, throttling etc.) but allows room for innovation in the form of specialised services. Securing enhanced quality characteristics will have a very important role to play to realise the full innovation potential of the IoT.

4. Degree of openness: open standards and interoperability

The IoT, like the internet, is a network of networks. While you may have a smart meter at home as well as a bio sensor, they have no need to communicate, are

[13] 'Proposal for a Regulation of the European Parliament and of the Council laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent, and amending Directives 2002/20/EC, 2002/21/EC and 2002/22/EC and Regulations (EC) No 1211/2009 and (EU) No 531/2012', European Commission proposal and text as amended by the European Parliament, 2013-2014: http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2013/0309(COD)&l=en

managed (and belong) to different entities and while one can be attached to a private infrastructure the other may go over the public internet. There are different requirements for closed critical networks (e.g. utilities) than open networks (e.g. monitoring parking space availability).

As such, the IoT is a useful overarching term, but does not reflect the multiplicity of different architectures. Nevertheless, internet protocol (IP) is becoming the common language for most data communication. Proprietary networks are migrating to IP in sectors such as the electricity grid, building systems, industrial manufacturing and oil systems. Enterprises are recognising the value of interoperability and scale, while IP networks have evolved to handle reliability demands.

To maximise the potential of the IoT, we need to further break down the silos between technologies in order to unlock the value for the economy and society. Agreeing on a wide range of open standards maximises economies of scale and simplifies education requirements. Open standards are key to driving interoperability, and the consequent benefits for the quality and capabilities of analytics. Cisco is committed to this goal, and together with other major industry players launch the Industrial Internet Consortium[14] earlier this year to help make it a reality.

The widespread adoption of IoT will require inexpensive devices that implement communications-related interoperability standards (examples include Zigbee, Wi-Fi, and LTE). For example, adoption of smart water and power meters that can communicate usage information to a utility through a cellular network will be discouraged if the addition of the cellular modem to a meter significantly increases the cost of the meter to the utility or ratepayer. There are some promising recent developments in the UK courts and in the European Commission regarding limiting the ability of owners of patents essential to implement telecommunications interoperability standards to compel payment of super-competitive licensing terms by wielding the threat of injunctions and other

[14] http://www.iiconsortium.org/index.htm

prohibitive orders.[15] This remains an area that merits continued attention from Ofcom and competition enforcement agencies.

A related issue is the stacking of royalties for patents required to implement interoperability standards, which may form a significant cost barrier to the widespread adoption of IoT by utilities, public authorities, and others. Implementing standards such as Wi-Fi or LTE may require licenses to hundreds or thousands of patents. As patents are increasingly acquired by non-practicing entities whose only business is patent licensing, more patentees owning patents required to implement interoperability standards focus on maximizing royalty income rather than, for example, defensive use of patents. This threatens to make patent licensing costs a barrier to adoption of IoT solutions. Successful IoT deployments may require the purchase of thousands or millions of devices, for example to sense traffic patterns in Greater London or power flow across the electrical grid of a UK distribution network. Clarity around licensing costs will facilitate widespread implementation of standards, and uncertainty around licensing costs will discourage it.

The international nature of the IoT development is likely to require a global standards approach. The nature of the IoT development also demands attention to wide-ranging standards and differing types of standards, including technical, application, quality and compliance standards. Standard setting should be driven by industry using current standard development organisations (SDOs) with the aim of setting a global framework. IETF will be a key SDO in ensuring that protocols are developed that do not adversely impact the internet. That said, there are a number of SDOs and industry forums engaged here, such as ATIS, CEN, CENELEC, Continua Alliance, ETSI, 3GPP, IEC, ITU-T (SG13 for y.IOT work), IEEE, IPSO, OneM2M and W3C. The layered model of networking shows that you need

[15] Case No. AT 39985 *Motorola—Enforcement of GPRS Standard Essential Patents*, DG Competition 2014:
http://ec.europa.eu/competition/antitrust/cases/dec_docs/39985/39985_928_16.pdf
A helpful discussion of the interplay between patents, standards, and competition law is provided in a recent report by the International Telecommunications Union, available here:
http://www.itu.int/en/ITU-T/ipr/Pages/Understanding-patents,-competition-and-standardization-in-an-interconnected-world.aspx

people working on lower layers, others considering applications, data format, interoperability and so on. As such, we do not believe that a single SDO will dominate this space, rather multiple groups will continue to be involved.

The role of regulators should be to encourage the development and adoption of open standards in this field, and foster interoperability. While standard development should be encouraged to mature in existing global SDOs, policy makers should encourage SDOs and enterprises to take an open and transparent approach, including, as noted previously, in relation to the rules they adopt regarding when injunctions are available to owners of patents required to implement standards and regarding licensing terms for such patents.

Ofcom's role:

- Encourage platform competition;
- Support greater use of public-private partnerships and examine new financing models to foster next generation access networks and transition to fibre;
- Continue to take a reasoned approach to net neutrality that allows for network management and intelligence in the network to the extent that it is not anti-competitive and advocate that in the European arena;
- Encourage the development of open standards and foster interoperability;
- Work with competition authorities to monitor and counter aggressive patent behaviour in forcing excessive licence payments for standard essential patents and examine the role of patent licensing costs as a barrier to IoT adoption.

5. Spectrum requirements

The consultation document correctly notes that the spectrum needs for IoT networks are heterogeneous due to the varied operational requirements of the networks. The paper rightly recognises range, sensitivity to quality of service, connection speed and duty cycle, device cost and battery life, network openness and security as crucial factors. As a result, both licensed and licence-exempt

spectrum will play important roles, wider and narrower channels, lower frequencies and higher ones. Such bands will indeed be complementary to one another.

From the rapid growth in traffic and number of devices outlined above it is easy to divine that there will likely be additional pressure on spectrum resources. The point we would like to address below, however, is that thanks to the range of connection types and the changing technology mix between them, the spectrum bands in question will not be identical in nature.

Ofcom notes that wireless is preferred for many IoT applications, but that is not the same as saying mobile. According to the VNI data, of the 480 million devices connected by 2018 in the UK, 33% of them will be mobile.[16] Looking more specifically at M2M connections, of the 7.3 billion global M2M connections in 2018, 2 billion will be mobile.[17] While these figures do not break out what proportion of the remainder will be fixed-wired or fixed-wireless connections, it is clear that while mobile will play a very important role, there is space alongside it for other wireless access methods such as Wi-Fi or mesh networks[18].

Within mobile M2M connections, we will see a change in the technology used. In 2013, 2G networks were clearly the go-to technology for mobile M2M with 71% of device connections.[19] 3G was 28% of connections and 4G less than 0.5%. In 2018, however, 3G will have surpassed 2G, with 51% of connections against 35%, while 4G will be making headway with 14% of mobile M2M connections.

In terms of specific bands, Cisco congratulates the UK on making the 870 – 876 MHz and 915 - 921 MHz available on a shared, licence-exempt basis. The band has particular advantages in that it is otherwise relatively lightly used, is proximate to the 863 – 870 MHz SRD band and because 915 – 921 MHz has a

[16] VNI Global IP Traffic Update 2013 – 2018 *op. cit.*
[17] VNI Global Mobile Data Traffic 2013 – 2018 *op. cit.*
[18] Cisco distinguishes between mobile, fixed-wired and fixed-wireless. Mobile covers mobile access technologies such as GSM, UMTS or LTE Advanced; fixed-wired accounts for when the device has a wired local access, such as Ethernet, whereas fixed-wireless accounts for wireless local access network technologies, such as Wi-Fi.
[19] VNI Global Mobile Data Traffic 2013 – 2018 *op. cit.*

strong international profile outside Europe, making it attractive due to existing equipment and economies of scale. The UK is pioneering the opening of this spectrum in Europe, and we urge Ofcom and the government to encourage their peers across the EU to follow suit.

Wi-Fi will be useful for IoT applications. With the technological developments inherent in the 802.11ac standard come the need for wider channels (80 and 160 MHz) and more spectrum. At the same time, the amount of IP traffic traversing over Wi-Fi will grow more than two and a half times between 2013 and 2018 in Western Europe, being the access technology of choice for 56% of traffic by the end of that period. The current spectrum allocation is insufficient to effectively meet the technological developments and the demand over the next decade and hence we support a contiguous band from 5150 – 5925 MHz for RLAN use on a shared basis. Following a European Commission mandate, sharing studies for the extension of the 5 GHz band are currently being developed in CEPT. We appreciate the support of Ofcom in helping to determine effective conditions and means to share with incumbent users and in convincing other regulators of the potential of such shared use.

For mobile, we support further consideration of bands for mobile broadband use. These include the ongoing processes to open up the 1.5 GHz and 2.3 GHz bands, as well as examining the potential to use the 700MHz band.

It is important that regulators continually assess the need for additional short-range device (SRD) spectrum bands to accommodate the IoT explosion. As the CEPT report 14[20] indicated in 2006 in response to a European Commission mandate on wider SRD use, we need to:

- Take advantage of the full opportunity for sharing spectrum
- Specify the minimum necessary regulations for use
- Remove application specific constraints, to the extent feasible
- Situate new bands adjacent or nearby to existing ones

[20] Report 014 Develop a strategy to improve the effectiveness and flexibility of spectrum availability for Short Range Devices (SRDs), CEPT, 2006 http://www.erodocdb.dk/docs/doc98/official/pdf/CEPTRep014.pdf

A further element is key not only for SRD bands but for all the wireless technologies mentioned above. In order to truly scale, new bands need to be similarly allocated globally. As such, harmonization at the European and international levels is paramount.

Finally, where spectrum bands are designated for sharing on an equal basis, as a general rule politeness between applications should be encouraged instead of favouring one over another. A current example of where this is playing out is for industrial automation in the Wi-Fi bands. Unless designated for exclusive use, primacy of an application, incumbent or otherwise, should be the exception rather than the rule.

Ofcom's role:

- Encourage European peers to follow the UK's lead in making the 870 – 876 MHz and 915 – 921 MHz bands available to use;
- Help determine effective conditions for Wi-Fi to share with incumbent users in an extended 5 GHz band and seek further understanding from colleagues in CEPT, RSC and RSPG in particular for this course of action;
- Maintain active support for additional mobile bands, including 700 MHz, 1.5 GHz and 2.3 GHz;
- Work with European peers to assess additional SRD bands and remove application specific constraints in existing ones.

6. Security and resilience

In order for the IoT to reach its potential, customers and end users must trust it. Both private sector actors and policy makers have the same ambition to ensure systems are secure and data protected. With more and more connections and a greater dependence of the economy and society on those connections, policy makers are justified in demanding security takes central stage.

Organisations operate in a changing threat landscape, seeking to stay one step ahead of potential threats and need flexibility in order to react. We must take

technical and organisational measures appropriate to the risk presented to secure the services.

Industry has long been working in partnership with governments, public authorities and other private sector actors at the national, European and global level to lead the fight for a secure cyberspace. At the heart of good security lie many of the practices and tools we have been building up over the last years. These include bidirectional voluntary information sharing; effective enforcement tools; incident preparedness, including cyber exercises; awareness raising and training; agreeing international norms of behaviour and development and recognition of international standards and practices. We should not stand still, however, and we welcome efforts to further support such activities.

M2M networks potentially open up new vectors for attack, and as with other developing technologies specific networks no doubt present specific challenges. From a regulatory standpoint, however, it does not make sense to subject the IoT to a separate regime. Regulation should be outcome-oriented as opposed to focusing on underlying technologies. As such, stricter security makes sense if there is a high risk of significant economic or societal damage. M2M is implicated to the extent it is used in high-risk scenarios and according to its vulnerability, it is not a valid target to regulate in and of itself.

When it comes to security regulation in general, whether for the IoT or not, we believe there are three key elements that should illuminate our approach. First, that security does not stop at borders – both threats and solutions are global in nature. Second, we operate in a rapidly changing threat landscape – and we need the flexibility to adapt to it. Third, total security is neither possible nor, given the associated costs, desirable. Security needs to be appropriate to the risks presented.

Cisco believes that regulating the security properties of products involved in the IoT would prevent security innovation to keep up with changing threats and isolate the UK and Europe from a global approach to such issues. Secure development, product assurance and evaluation are already, and should continue to be, addressed through methods such as the Common Criteria (ISO 15408),

which is recognised by governments around the world[21]. We also believe that legislation is not the best way to approach vulnerability disclosure. International standardisation activities are currently taking place and this process should not be preempted and locked down in legislation, which is difficult to amend and regional. Finally, we believe that introducing liability for software producers would significantly impair both innovation and security and could lead to software being dominated by a few huge vendors that would accept liability for a very narrow usage or a thriving and innovative economy with cheap or free software. The UK government has been supportive of this stance in the negotiations around the draft EU Network and Information Security (NIS) Directive and we encourage them to continue this approach[22].

In terms of Ofcom's role, Article 13a of the European Framework Directive only relates to a subset of networks involved in the IoT[23]. While we noted above the important role mobile operators and other public electronic communication network and service providers play in the IoT, other networks fall out of the scope of this legislation. Other organisations that might make use of IoT networks and applications are subject to different regulatory oversight for security (e.g. financial services) and European legislation is in the pipeline that potentially establishes further duties and responsible bodies (the draft EU NIS Directive). Ofcom needs to coordinate as appropriate with the other authorities and recognise the limits of its own responsibilities.

Ofcom's role:

- Continue security oversight role for public electronic communication network and services but recognise scope limits;
- Share information and coordinate with other competent authorities and operators if and when the EU NIS Directive is adopted;

[21] https://www.commoncriteriaportal.org

[22] 'Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union', European Commission proposal and text as amended by the European Parliament 2013 – 2014: http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2013/0027(COD)&l=en

[23] For further information about the scope and nature of the Article 13a provisions, please see the guidelines produced by ENISA's Article 13a Expert Group: https://resilience.enisa.europa.eu/article-13

- Support the positive approach taken by the Department of Business, Innovation and Skills in the discussion on the NIS Directive;
- Encourage security awareness raising and training initiatives and engage in them as appropriate.

7. Data privacy

Alongside security, the other element of customer and end user trust is privacy. The unprecedented social and economic benefits of the IoT do not need to come at the expense of privacy, and can be realised in a responsible manner. But it is important that end users know about how their data is used and feel comfortable about it. The IoT implies greater use of data for positive ends, but also with the potential to leave citizens feeling exposed if not handled correctly.

Not all data is created equal, of course. Many M2M use cases, such as agricultural sensors checking on weather and soil conditions, do not involve the processing of personal data at all. Of those that do, data can be sensitive or low-risk. We are more concerned about how and whether data about our ethnicity or sex life is being analysed than data about, say, our shoe size. Moreover, the context of how data is being used is important – which is why intention and outcome are important to how we regulate processing of data. The combination of sensors and analytics using location data to implement crowd management in an airport, for example, is clearly in the interest of the individuals in question; but we might feel more uncomfortable if an oppressive regime is using technology to track the location of dissidents.

The IoT clearly raises new questions as to how data protection frameworks can be applied and we need to get this right in order to both enable the IoT to flourish and protect personal data. On the one hand, in the European framework explicit consent will remain a key method for giving users control over the use of their personal data. In using analytics to connect patients' health data and improve health provision, for example, citizens should be given a choice whether they want such sensitive data to be connected. On the other hand, particularly for M2M devices, the lack of user interfaces on sensors means that checking boxes

on paper or digital devices will not always be possible, and we will need to consider other ways of giving consent and alternative legal bases for processing such data.

In the IoT, the data collected by the connected devices is an essential part of its value. It depends on the ability to cross-reference data and analyse it in new ways, as well as tailoring to individuals. As such, data protection frameworks need to be careful not to vilify profiling that is calibrated to user expectations and is otherwise appropriate and beneficial to individuals; and methods to enable reuse of data may need to be updated.

Moreover, while certain data will remain within closed networks or behind firewalls in specific data centres, the IoT also implies that many data will travel and be processed across borders. As such, we need to make sure that we have usable mechanisms for handling international data transfers and for addressing issues relating to data sovereignty that do not put companies in the impossible situation of being required to comply with conflicting jurisdictional requirements.

Current frameworks are not always best placed to enable this new world. The EU is known for its strict approach and is currently updating its framework[24]. Negotiations are so far not solving these issues but introducing prescriptive, rigid rules and adding new layers of administrative burden that impede innovation.

As Ofcom notes, the primary body for implementing the privacy framework is the ICO in the UK, whereas the Ministry of Justice and various government departments are engaged in developing the new EU framework. Nevertheless, we welcome support in recognising that the rules we create for the use and protection of personal data are essential to the success of the IoT; we need a

[24] 'Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)', European Commission proposal and text as amended by the European Parliament, 2012 – 2014: http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2012/0011(COD)&l=en

harmonised framework that embraces innovation and allows Europe to reap the benefits of this new era.

Ofcom's role:

- Champion the role of a workable and innovation-friendly data protection framework in the successful development of the IoT. Work with the Ministry of Justice to advocate this position among European policy makers.

8. Numbering and addressing

There is no doubt that IPv6 will be the internet protocol for IoT. With 12 billion connected devices as of last year and only 4.3 billion IPv4 addresses, many devices already have to share IP addresses. The stock of IPv4 addresses has simply run out. The Internet Assigned Numbers Authority (IANA) ran out of addresses to delegate to Regional Internet Registries (RIRs) in 2011, and three of the five RIRs have already exhausted these stocks, including RIPE NCC, which covers Europe.[25]

IPv6 is beyond the realms of foreseeable exhaustion. There are enough addresses for every atom on the surface of the Earth to have 100 addresses.[26] Transitioning to IPv6 will allow the IoT to continue to grow and prevent address exhaustion from acting as a bottleneck, squeezing new innovation.

There are three main elements to consider when assessing the switch. First, are the devices ready, second, are websites publishing IPv6-enabled content and third, are internet service providers provisioning IPv6.

In terms of device readiness, in the UK, there will be 310 million IPv6 capable fixed and mobile devices by 2018. This is up from 86 million in 2013 and represents a 29% compound annual growth rate (CAGR). As such, 64% of all networked devices in the UK will be IPv6 capable in 2018, up from 31% last year.

[25] See, for example: http://www.potaroo.net/tools/ipv4/
[26] Comparison attributed to Dick Guertin by Steve Leibson: http://www.edn.com/electronics-blogs/other/4306822/IPV6-How-Many-IP-Addresses-Can-Dance-on-the-Head-of-a-Pin-

It is worth noting that legacy devices not supporting IPv6 will not cease to function with the transition to IPv6 as service providers will not 'turn off' IPv4. Moreover, natural device churn will accelerate the transition. In this sense, the transition will be somewhat organic and there are the opportunity cost for citizens is negligent.

In terms of content, 45% of webpages are available over IPv6 in the UK. This is within 10 percentage points of most other peers in Europe and North America, though the UK is at the lower end of that range. One notable exception is the Czech Republic, where 62% of websites are IPv6 enabled.

The number of actual users is much lower than the proportion of devices and content that is ready. According to a Google tool that measures the percentage of users accessing their services over IPv6, 4.3% of total global access is over IPv6.[27] This is certainly moving in the right direction, having increased from 1.7% at the same time the year before. The statistics are not so good in the UK. While Europe could in many ways be seen as leading the path to adoption, in the UK, the amount of IPv6 traffic is just 0.21% of the total. This contrasts against 5.5% in France, 9.6% in the US, 11% in Germany and 29% in Belgium, the world leader.

Service provider adoption seems to be driven by the desire to innovate, with service differentiation and reduced operational complexity. If you look at individual service providers' rates of deployment, where they are deploying IPv6, they are doing so at breakneck speed. Verizon Wireless, for example, has reached over 50% of its user base in less than 24 months.[28] What this shows is that IPv6 adoption is an operator driven migration, and that contrary to common opinion, it can be very rapidly if done *by default*, without expecting the end-user to opt-in.

Policy makers need to champion IPv6 adoption in networks, devices and websites, and promote more IPv6 enabled content, local content in particular. They should lead by example through adoption by public services, as well as conducting awareness raising and training. Another key challenge is the knowledge gap as there is a lack of IPv6 education at technical schools today.

[27] Google IPv6 tool, figures for 24 August 2014: https://www.google.com/intl/en/ipv6/statistics.html
[28] See http://www.worldipv6launch.org/measurements/

Ofcom's role:

- Encourage and enable service providers to deploy IPv6 by default;
- Encourage government departments and the public sector to lead the way in public sector adoption;
- Conduct awareness raising and facilitate training programmes;
- Work with the private sector to promote IPv6 education in technical education institutions.

9. Digital literacy

The IoT will revolutionise many sectors that have not been traditional leaders in leveraging information and communication technologies. As such, as important as digital literacy of citizens undoubtedly is, we see the skills issue as broader. New competences will be required of the labour market, be it entrepreneurs launching new services and solutions, designers of networks or those installing them.

Cisco's Networking Academy – which is currently teaching ICT skills to more than one million students worldwide – is well aware of the issue.[29] NetAcad is a public-private partnership model via which Cisco provides free of charge curricula, virtual learning tools, instructional support, teacher training and professional development opportunities for instructors. We partner with educational institutions, nonprofits, NGOs, and community centres. Over 1.2 million students have taken NetAcad courses in Europe since its inception and we intend to train at least 1 million more over the next five years. In the UK alone we have over 230 academies.

As an example of our response to the demand for IoT skills, we have developed a new smart grid curriculum to provide internet protocol competences for electricians. A pilot in Germany has already established the course content and training of teachers has already begun. The curriculum is now set to be tailored and disseminated more broadly, starting with the UK and three other European

[29] Find out more about Cisco Networking Academy at https://www.netacad.com

countries. As a result, we expect to train up to 5000 students in the pilot classes and in excess of 100,000 by the 5th year.

Policy makers need to encourage the public and private sector to work together to address the impending skills gap, as championed by e-Skills UK and the Tech Partnership in the UK; raise awareness through campaigns such as the European eSkills Week and recognise industry certifications in formal education qualifications.

Ofcom's role:

- Engage in and support awareness raising campaigns and skills initiatives;
- Encourage appropriate UK government departments to recognise industry certifications in formal education qualifications.

10. Big Data: data analysis and exploitation

The ability to 1) gather, process and analyse data in a way that makes it meaningful and 2) get the right information to the right person or machine at the right time are intrinsically part of the ecosystem of the IoT.

90% of the world's stored data was created in the last year alone.[30] At the moment, however, most data is unstructured and underutilized. Only 0.5% of all data is currently being analysed for insights.[31] Applying analytics to a greater share of current data could lead to productivity improvements, economic growth and societal developments.[32]

As such many of the policy and technical issues that are important for the IoT similarly apply to big data. Core issues already touched upon in this response include standards and interoperability, privacy, security, spectrum, bandwidth constraints and device/ computing requirements.

[30] IBM Research, 2013, quoted on website: http://www-01.ibm.com/software/data/bigdata/
[31] 'The Digital Universe in 2020', IDC iView, J Gantz and D Reinsel, 2012. Sponsored by EMC
[32] For a more developed and evidenced argument, please see 'The Internet of Everything: How the Network Unleashes the Benefit of Big Data', Chapter 1.2 of the Global Information Technology Report 2014, R. Pepper and J. Garrity (Cisco): http://blogs.cisco.com/wp-content/uploads/GITR-2014-Cisco-Chapter.pdf

An additional policy area for data exploitation is that of opening up public sector data resources for use. According to Open Knowledge, the key attributes for openness are availability and access, reuse and redistribution and universal participation.[33] In other words, to be truly open it is not enough that one can ask to see the data, it must be available as a whole, at a reasonable reproduction cost (preferably free), preferably over the internet and in a convenient form. It should be machine-readable, such that it has open APIs, and under terms that permit reuse and combination with other data sets. It should be open to all to use and distribute with no limits on particular purposes or restrictions on commercial use.

The UK is clearly in a leading role when it comes to open data, as recognised by the Open Data Index.[34] Nevertheless, there is always more work to be done. This includes the number of datasets made available, at national but also local level; ensuring data is licensed on open terms and to ensure data is kept up-to-date.

Ofcom's role:

- Support the Cabinet Office in championing further opening further data sets on open licensing terms and make the connection to Big Data.

11. Impact of sectoral regulation

A final topic that Ofcom does not directly address is the impact of sectoral regulation. The IoT will transform many economic sectors, including those that are highly regulated. We do not claim expertise in many of these sectors, nor is it within the remit of this consultation, but nevertheless there is the possibility that significant revisions in regulatory approaches might be appropriate. In healthcare, for example, rules about remote consultation might need to be updated or food regulation internationalised to account for a smart, global food supply chain.

Individual regulators may be examining the issues, such as Ofgem and DECC's Smart Grid Forum. Nonetheless, this is likely to be happening in a piecemeal

[33] Open Knowledge website: https://okfn.org/opendata/
[34] Open Data Index, 2013: https://index.okfn.org

fashion, and there may be a role for Ofcom or another body to coordinate efforts to examine regulatory barriers across various sectors and ensure that expert groups are established in order to identify and dismantle them.

Ofcom's role:

- Coordinate the assessment of regulatory barriers to the IoT across various industry sectors.

Conclusion

Cisco embraces the broader concept of the Internet of Everything, which includes things but also brings people, process and data into play. As a result, we examined the differences in definition and demand for both IoE and IoT at the beginning of the document before reverting to the narrower concept of IoT for the policy questions in line with Ofcom's enquiry. Both the IoE and M2M connections within it are subject to explosive growth and will bring significant economic and social value. Healthcare, transport, energy, retail and manufacturing are all well set to gain from it if they seize the opportunity in front of them. Shrinking form factors, advanced computing, the mutually beneficial development of cloud, mobile and big data as well as a shift in business creation drive the growth of IoT.

In terms of policy issues, traffic growth dictates the need for greater network bandwidth and hence there is a need to create the right policy framework to stimulate investment in a higher speed and more robust broadband network. Intelligence in the network is equally important, however, and net neutrality rules must be correctly framed. While the IoT is a network of both closed and open networks, in order to maximise its potential we need to adopt open standards in existing global forums. The spectrum needs for IoT are heterogeneous and need to constantly assessed to ensure that this does not act as a bottleneck to the development of the IoT.

Security regulation should be outcome oriented and hence IoT specific regulation is inappropriate. Nevertheless, we need to get the general security framework right and encourage joint activities between the public and private sector. It will also be necessary to adopt data protection rules that allow the IoT to reach its potential, as its value is dependent on the ability to cross-reference or reuse data in new ways.

IPv6 is the addressing system for the IoT and we need to ensure all parts of the ecosystem are adopting it. The IoT will create new demands on the workforce and the public and private sector will need to work together to ensure we are prepared. Given they go hand-in-hand, the issues for big data are at heart the same as for IoT. An additional issue, however, is the recommendation that policy makers pursue open data practices. Finally, a review of regulated sectors should be coordinated to ensure there are no sector-specific rules impeding IoT development.

Ofcom clearly has an important role in developing and implementing policy that will help the IoT to thrive and will take a clear lead in spectrum, network-related issues and addressing. But as Ofcom itself recognises, many different actors need to be involved in getting the policy framework right. As such, part of Ofcom's role will be to ensure that there is a clear vision in relation to various disparate policies, and that the bodies taking the lead on those topics recognise the importance they have for Europe's economic and social future in the IoT era. This will involve working together with various government departments but equally as important in convincing international peers, particularly in Europe. In essence, Ofcom needs to be a champion for the IoT and we welcome this consultation as the first step on that road.

* * *

Cisco looks forward to continue working with Ofcom as it examines how to promote innovation and investment in the IoT space. For any questions or additional information regarding this submission, please contact:

Chris Gow
Senior Manager, Government Affairs
Cisco
Phone: +32 2 704 1573
Mobile: +32 494 653 104
chgow@cisco.com

or

Ian Foddering
Chief Technology Officer & Technical Director
Cisco UK
Phone: +442088249358
Mobile: +44780878429
ifodderi@cisco.com