Huawei response to Ofcom request for input on "Promoting investment and innovation in the Internet of Things (IoT)"

INTRODUCTION

Huawei welcomes the opportunity to express its views on the role of Ofcom in the evolution of the Internet of Things. We agree with Ofcom's comment that IoT will be a major driver of investment and innovation in the communications sector in the years to come. The benefits will affect all our lives in one way or another.

A favourable regulatory environment will be needed to ensure that the immense opportunities that will result from the IoT will be taken up and positively impact UK businesses, citizens and the UK economy.

IoT definition, applications and demand:

It is very difficult to come up with one definition of the IoT because there will be such a wide range of uses and deployments. The end result would be a generic definition of little practical use.

It is also too early to forecast which applications are likely to dominate. We would anticipate that within 6 to 12 months a picture will start to emerge on the market directions and we will then be in a better position to start forecasting with more certainty..

A very recent (September 2014) Analysis Mason report[1] on low-powered wireless solutions investigates the challenge to telecoms engineers to produce a low-power, wide-area (LPWA) network that can connect to modules that require a single AA battery for 10 years of life and that will cost under USD5 each. This paper also looks at the potential market and opportunities for such a solution.

[1] http://www.analysysmason.com/Research/Content/Reports/Low-powered-wireless-solutions-have-the-potential-to-increase-the-M2M-market-by-over-3-billion-connections/

Within this report there are references to a Neul/Huawei initiative on "Cellular IoT radio access"[2] which has been proposed for standardization in 3GPP GERAN. This initiative will be of interest to Ofcom.

Spectrum requirements:

Huawei supports the harmonization of the 694-790MHz band, and the achieved agreement on the 2*30MHz frequency arrangement, aligned with the 3GPP band 28, within CEPT was a major achievement. The actual utilization of spectrum outside of the 2x30 MHz blocks should be a national decision, bearing in mind the differing views from administrations on this.

Huawei believes that the UK proposal to the last meeting of ECC PT1 to study the option of a frequency arrangement of 2 X 3MHz suitable for M2M, comprising 788-791MHz for downlink paired with 733-736MHz for uplink (ECC PT1(14)106), was a positive step forward. This proposal was agreed by ECC PT1 (Section 7.3 and Annex 20 of the draft minutes). (It is expected that the proposal will be re-presented to ECC PT1 #48 in January with additional wording to ensure technological neutrality i.e. not based on the characteristics of a particular technology being developed for this application.)[3]

Currently it is very difficult to predict the future spectrum requirements for IoT.

- We believe that there will be two categories, i.e. licensed and license-exempt
- Licensed will be used where a guaranteed quality of service is needed.
- European/international harmonization is required where ever practicable and possible to ensure device economies of scale.
- The UHF bands are preferred because of their suitability for IoT connectivity

Security and resilience:

Amongst others, one of the main IoT characteristics will be the fact of having little manual intervention and handling of humans when it comes to initializations, installation, deployment, configuration and usage of IoT devices or services. Automation will be key enabler in this field and it will most likely be considered positive that interactions with IoT devices and service cannot be observed, unless specific inspection is performed deliberately. Basically the tendency is to have IoT devices providing useful services, but their existence shall not be perceived. As a consequence users will have less control over IoT devices and may not even notice the existence of these devices.
A second main IoT characteristic is device size: there's the tendency that devices get smaller and smaller thus also supporting to be less visible and perceivable by the human users. When things get smaller, they also tend to have fewer resources that can be used. From a security and privacy perspective this will most likely impact the computation power, storage capabilities and available electrical power, e.g. needed for communications.

[2] http://cwbackoffice.co.uk/Presentation/Wirelessly_Connecting_IoT_19.06.14_RobertYoung.pdf

[3] Ofcom IFPG WGD (14) 078

Challenges encompass:

- Cryptographic mechanisms that are strong enough despite restricted computational capabilities and limited power supply.
- Low cost, yet preferably hardware based root of trust, like e.g. physically unclonable functions.
- System integrity solutions that work on small scale and yet have update capabilities, avoiding deployed IoT devices avoiding having long term security flaws.
- Solutions that integrate reliably and auditable into backoffice or cloud systems as most of the data processing and analysis will happen outside IoT devices.
- Standards that address interoperability concerns and have applicable and suitable security properties encompassed for the beginning

Huawei would also like to bring to Ofcom's attention a very recently adopted Opinion (Opinion 8/2014 on the Recent Developments on the Internet of Things[4]) from DG Justice which we believe supports the comments made above and also in the subsequent section on Data Privacy.

Data privacy:

IoT poses many challenges in data protection, given the myriad uses of personal data, many of which will be collected passively via systems and sensors invisible to humans. In the emerging IoT environment, the individual is often unaware of the data collection taking place or may be completely absent from the transaction being processed. This poses extra challenges in satisfying basic data protection principles, like "Notice and Choice" as well as "Purpose Specification and Use Limitation". This might lead to proposals suggesting relaxing the requirements on data collection and giving more emphasis on ensuring accountability by data users/controllers instead. This would mean taking a paternalistic approach, where the burden of privacy protection is shifted away from individuals and towards data controllers.

However, reducing individual's control over their personal data has always led to great privacy abuses and cannot work as a solution for better privacy protection. Addressing the new challenges in IoT should not mean moving away from a user-centric approach, where the individual – the data subject – ultimately determines the fate of his or her personal data.

[4] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

Therefore, it is our position that:

- The ability of individuals to exercise meaningful control over their personal data should be protected and enforced through the application of Privacy by Design, which proactively embeds privacy into information technologies, business practices and network infrastructures.
- De-identification, pseudonymization and anonymization are virally important tools to protect privacy, by reducing the risk that personal information is used for unauthorized or malicious purposes. This should be done in a way that the risk of re-identification is minimized, while ensuring a level of data quality that is appropriate for secondary uses.
- Emphasis should be given on technical innovation in privacy-enhancing and transparency-enhancing technologies to enable individuals manage and control their personal data more intuitively and effectively that is currently possible.

Numbering and addressing:

A new "Named Data Networking"[5] (NDN) consortium had been formed which is aimed at developing a new system of connectivity that promises a future without servers or IP addresses.

"Named Data Networking (NDN) is a potential Internet architecture designed as a distribution network. To access the NDN network, a user needs to install some software applications and the protocol stack. This serves as a software router, working together with a core component of the network, the NDN Forwarding Daemon, to allow communication without IP addresses or hardware servers."

If this project becomes reality, in the long term it may have major relevance for device addresses.

Devices:

The references refered to in the 'IoT definition, applications and demand' section also cover the views requested here.

Data analysis and exploitation:

Big data and IoT are tightly linked as the data captured from the devices is the source for the Big Data paradigm and definition. Such a paradigm is currently beingstudied within standardization bodies. ISO/IEC JTC1 has set up a study group in November 2013 in order to develop a guiding report on the standardization work items and issues, and also performed a gap analysis for Big Data. This report has just been finalized and will presented during the upcoming JTC1 Plenary in November 2014 in Dubai. This report will constitute a good resource for the information requested in this section. Also,

[5] http://named-data.net/consortium/

within ISO/IEC JTC1, a similar study group has been set up for IoT, a close coordination and collaboration will take place in the future between the working groups develoing work items related to these two topics.

International developments:

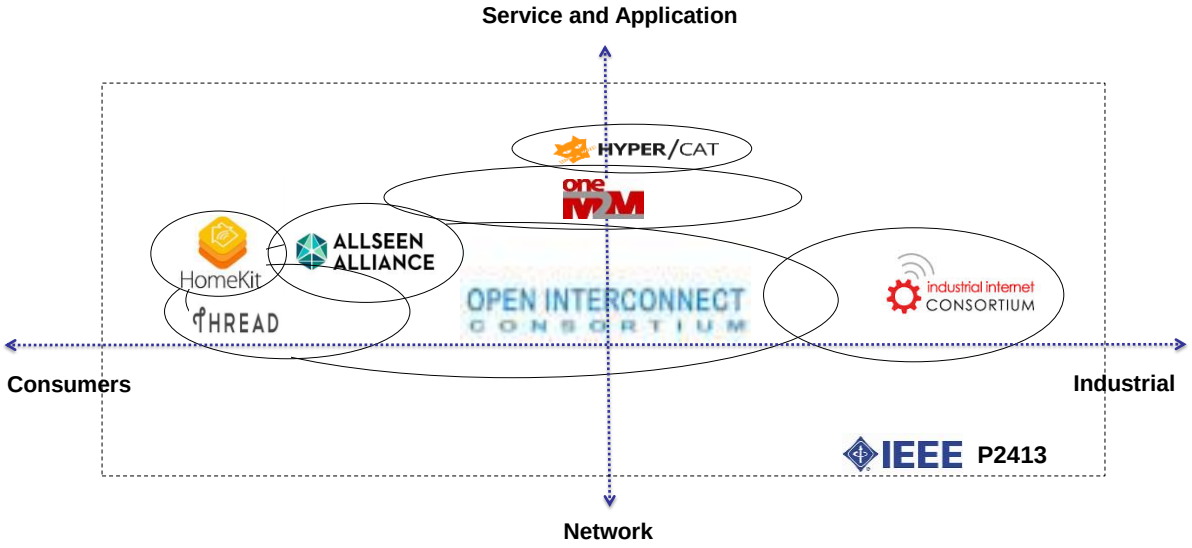
Consortia activities

The number of consortia performing standardization and other activities relating to IoT is increasing on what seems like a weekly basis. Huawei's expectation is that the path being followed will be similar to the wave of activity following the advent of Cloud Computing around 5 years ago i.e. wide ranging work progressing through a mix of existing and newly formed consortia, Partnerships, and formal standards organizations. Following this, again within 5 years,we expect a rationalization and consolidation of these activities as the standardization requirements of specific sectors and vertical industries are satisfied.

Examples of consortia engaged in IoT activities			
Industry Internet Consortium	Industries 4.0	HyperCat	Innovation Alliance of Industry and Internet Convergence (China)
IETF	AllSeen Alliance	OneM2M	HomeKit
Thread Group	Open Interconnect Consortium	Global Platform	OGC

The IoT Organization Landscape below gives a generalized picture of how some of these consortia and partnership activities fit together in the bigger picture of IoT.

IoT Organization Landscape



Using oneM2M as an example of the varied work being undertaken:
oneM2M is a large Partnership which includes ARIB, ATIS, CCSA, ETSI, TIA, TTA, TTC, BBF Continua Alliance, HGI, and OMA as members. Its work includes the development of the oneM2M services layer standard, and also encompases the following aspects:

- Availability of the first oneM2M Release (now in Public comment phase, under the form of a candidate release, will be published as Initial release in January 2015).
- A oneM2M showcase, with an expected seven demonstrations, originating from companies from the regions below, and related with different sectors (energy, health, home networks, automotive) will take place in ETSI in next December.
- oneM2M as global standardization initiative, covering Europe, China, Japan, Korea and US – which is comparable to the geographic coverage of 3GPP
- oneM2M develops standards for IoT services agnostic of any kind of the underlying networks - wireline, satellite, cellular or wireless – providing connectivity.
- oneM2M allows a diversity of companies to implement interoperable IoT platforms, which are essential fore ensuring both interoperability (and hence cost-effective deployment of the technology), however leaving open the implementation choice of service providers, when openness is the opposite of the approach to an IoT dominated by a small number of proprietary entities.

Formal standardization

As previously mention in the our response to the 'Data analysis and exploitation' section, ISO/IEC JTC1 has ongoing activity in study groups on 'Big Data' and 'IoT'. It also has a WG on Sensors and sensor networks.

Examples of formal standardization bodies engaged in IoT work		
ISO	IEC	ITU
IEEE	ISO/IEC JTC1	ETSI

The above examples are recognised SDOs (Standards Developing Organizations) that have a global out reach. There are of course regional and national SDOs that are also working on facets of IoT standardization.

EC/ETSI example

An EC initiative covering "Smart Appliances" being developed in conjunction with ETSI is an important one. The issue here is not a lack of standards. There are perhaps too many standards each dealing with a fragment of a topic, sometimes with existing overlaps. The "Smart Appliances" EC initiative is targeting the definition of a single reference ontology to cover the needs of all appliances relevant, for now, for energy efficiency; inter alia, depending on the success, in the future it might be expanded to cover other requirements. An EC related study is called "Available Semantics Assets for the Interoperability of Smart Appliances. Mapping into a Common Ontology as a M2M Application Layer Semantics"

In these examples of consortia, partnerships, and formal standardization activity currently being undertaken, which is considerable, we would not suggest that Ofcom gets involved with any of this activity but builds a mapping/scoping of these activities to assist its future directional thinking as IoT evolves.

The international dimension - US

The FCC are well aware of the impeding demands on spectrum with the explosion of IOT and know they'll need act at some point in time. In response, the FCC assigned the topic to its Technical Advisory Council (TAC) with the following Charter:

TAC IOT WG Charter:

- Identify key areas in the evolving Internet that should drive the work of the Commission or areas where the Commission should seek key information
- What new demands will the Internet of Things (including M2M) place on the network?
- What technology policy challenges exist in the evolution towards an Internet of Things?
- Explore how the FCC can foster IoT innovation and leverage Federally funded R&D in this area

IOT WG Actions (as of 6/2014):

- Developed Taxonomy of IOT by vertical segment
- Mapped standards activity relevant to IOT
- Generated initial findings and strawman recommendations related to spectrum & IoT security
- Identified Next Steps

IOT WG Spectrum: Strawman Recommendations: (Note: these may or may not be accepted)

- No unique allocations of spectrum to IoT are required [with the possible exception of short-range unlicensed spectrum that is subject to very high spatial reuse]
- The FCC should periodically and systematically refresh its analysis and plans to address spectrum demands associated with IoT to ensure there is:
  - Sufficient short-range spectrum to meet growth in PAN/LAN requirements arising from IoT
  - Sufficient capacity upstream from IoT Proxies to accommodate increased demand associated with IoT
- This analysis should take account of significant technical innovations and the resultant plans should be sufficiently concrete and timely as to guide industry planning related to IoT.
- Long-lived things should use short range unlicensed spectrum whenever a safe harbor from wireless technology evolution is required
- To stimulate IoT growth, the FCC should focus on the availability of unlicensed spectrum suitable to a range of PAN/LAN services (including, but not limited to IoT)

The international dimension – China

In 2013 an inter-agency council was established to coordinate the Chinese government's policy and action on IOT. The members include NDRC, MIIT, MOST, the Ministry of Education, and the National Standardization Administration. With the support of this council, China issued a Directive on IOT industry development and IOT Action Plan in 2013. The plan specified targets for the industry by 2015 in terms of top-level design, standards formation, technology R&D, application and promotion, industrial support, business models, safety, government support, laws and regulations, and workforce training.

When announcing a new GSMA report on 'How China is set for global M2M Leadership'[6] in June 2014, Alex Sinclair, Chief Technology Officer, stated:

"Proactive government support has benefited China and its mobile operators, whereas in many global markets, regulatory uncertainty has held back the deployment of M2M solutions.."

[6] http://www.gsma.com/newsroom/wp-content/uploads/2014/06/china-report.pdf

The report states that "At the end of 2013, China had 50 million M2M connections, ahead of the U.S. with 32 million and Japan with 9.3 million, according to Sylwia Kechiche, Senior Analyst M2M, GSMA Intelligence. The addressable market in China is immense and represents an incredible opportunity for continued future growth when one considers the sheer number of things that could potentially be connected."

In summary, it appears that the US and UK administrations are at the same stage of working to determine the requirements for a future successful uptake of IoT within their geographies. China is currently the clear leader from an M2M perspective and is in the process of moving from M2M to IoT

Ofcom's role:

Huawei belives that the role of Ofcom will be key to ensuring that industry is able to take advantage of this area. We are also aware that this will be an extremely challenging task for Ofcom to help provide a platform in its role as an enabler for the IoT to ensure a successful takeup of the opportunities and benefits that the IoT will present.

- Ensuring a favourable regulatory environment will be essential
- Ensuring sufficient availability of the appropriate spectrum for IoT needs (both licensed and license-exempt)
- Ensuring a defined QoS for the use of licensed spectrum in IoT
- Mapping of relevant standardization activities relevant to IoT
- Defining and developing its role as the guardian of consumer interests in this area

---