Internet of Things –
Just Hype or the Next Big Thing?

In a two part series James Halliday and Rebekah Lam take a considered look at the phenomenon of, and regulatory and policy issues that apply to, the Internet of Things. In this part they discuss the implications for the communications and content industries including what IoT means for the net neutrality debate in Australia.

There has been a tremendous amount written and discussed about the Internet of Things (IoT). Gartner recently reported that this phenomenon was at the crest of its annual "hype cycle", believing that the development of the IoT is subject to overinflated expectations and that its widespread adoption is still some years away.[1]

Gartner and others attribute this finding in part to a lack of standards between emerging IoT technologies, believing that the work towards common standards will continue for some time. While it is certainly true that a lack of standardisation presents a number of technical challenges in the uptake of the IoT technologies, it also creates unique regulatory challenges.

This article is the first in a two part series examining some of these policy implications in the context of this important emerging technology. In this part we look at some of the implications for the communications and content industries, including what the IoT means for the business models of carriers; interoperability and standards issues; numbering plan and roaming implications; and spectrum allocation policy. We also look at what the IoT means for the net neutrality debate in Australia. In part two, we will examine a range of issues for government and consumers arising out of the IoT.

WHAT IS THE INTERNET OF THINGS?

There is no widely accepted definition of the IoT. It has been variously described as "the third wave of the internet", "a scenario in which objects, animals or people are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction" [2], and as "the concept of basically connecting any device with an on and off switch to the internet (and/or to each other").[3] It has also been referred to as "physical objects that connect to the internet through embedded systems and sensors, interacting with it to generate meaningful results and convenience to the end-user community".[4]

The ITU has offered a typically dry definition of the IoT, stating that it is "a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies."[5] The ITU also notes that "through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled." Interestingly, the ITU goes on to say "from a broader perspective, the IoT can be perceived as a vision with technological and societal implications."

The inability to clearly articulate exactly what the IoT is and what it encompasses, underlies the complexity generated by its accelerating growth. This growth is producing ever increasing volumes of data, demanding more processing power and requiring more complex analytics. Some predict there will be at least 50 billion connected devices by 2020 (there are currently about three billion) with machine to machine communications generating at least US$900 billion in revenues by that time.[6]

> ***There is no widely accepted definition of the IoT.***

This surge in connected devices is sometimes described as the internet becoming "commoditised" or "industrialised" where the abundance of information about a person's attributes, preferences and behaviour is leading to the "datafication of society"[7]. Data can be captured, analysed and stored by data brokers who provide the information to private companies that use the information for marketing, product development and other business purposes. In this sense then, the IoT is part of a broader trend of big data analytics, which also presents many policy challenges similar to those posed by big data.

What is very clear is that the IoT is not homogeneous but extremely diverse and involves a

>

[1] http://www.theguardian.com/technology/2014/aug/12/internet-of-things-most-over-hyped-technology.

[2] http://whatis.techtarget.com/definition/Internet-of-Things

[3] http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/

[4] http://www.ey.com/Publication/vwLUAssets/EY-cybersecurity-and-the-internet-of-things/$FILE/EY-cybersecurity-and-the-internet-of-things.pdf

[5] ITU-T Y.2060 (06/2012) "Overview of the Internet of Things."

[6] http://www.ey.com/Publication/vwLUAssets/EY-cybersecurity-and-the-internet-of-things/$FILE/EY-cybersecurity-and-the-internet-of-things.pdf

> range of technologies with a wide array of applications for both individuals and businesses. Some of these technologies exist in industries more regulated than others (e.g. health and transportation) but some industries are not directly regulated by any industry-specific rules (e.g. exercise and diet trackers).

Any regulation of the IoT cannot therefore adopt a "one size fits all" approach but must take into account the complexity of the IoT environment. In some senses, the IoT is a purely incremental issue in the context of broader trends in the communications industry, while in others it also presents its own unique and formidable policy challenges.

It seems then that common standards are still some way off

RISKS AND BENEFITS OF THE IOT

The IoT provides tremendous value to users by offering convenient solutions that not only save time and money, but can also save lives and help governments allocate resources more efficiently. (In common with many other technologies, it also offers endless opportunities for mindless diversion)!

One of the most obvious and immediate challenges arises from the sheer and growing volume of IoT devices. This has many different aspects. Many IoT devices are typically low powered, relatively unsophisticated devices which transmit or receive packets of data intermittently. Individually, each device takes up a miniscule amount of total network capacity; however, together, these devices generate a considerable and growing amount of traffic across mobile and, commonly, fixed (usually via wi-fi) networks. Since this traffic is "device grade", it does not typically require access to consumer grade carriage services to operate. This means that many existing networks may not be optimally engineered for IoT traffic.

The future of the IoT is therefore dependant on robust infrastructure including ubiquitous fit-for-purpose broadband connectivity and sensor based technologies. There is an important practical question about whether these enabling technologies can keep up with the demand to successfully support the growth of the IoT.

As Gartner identifies, one key question is standards. An Intel IoT group senior vice president and general manager recently said, the "IoT is a significant opportunity but one that needs interoperability and scale to fulfil industry predictions of billions of connected devices".[8]

Different vendors are releasing different standards but there is as yet no common or prevailing standard. There are also global initiatives including the Open Interconnect Consortium (OIC). The OIC's purpose is to define a "common communication framework based on industry standard technologies to wirelessly connect and intelligently manage the flow of information among devices, regardless of form factor, operating system or service provider."[9]

OIC is the sponsor for the "IoTivity Project", an open source software framework enabling seamless device-to-device connectivity to address the emerging needs of the IoT. There are also many other standards bodies working on similar or related projects, including the ITU and the European Telecommunications Standards Institute. It seems then that common standards are still some way off.

THE TELECOMMUNICATIONS ACT 1997 (CTH)

In Australia, telecommunications is centrally regulated by the *Telecommunications Act 1997 (Cth)* (**Act**) and related legislation.

Operators of IoT devices will generally not (at least during the early stage of the IoT) be carriers or carriage service providers under the Act because they will not be providing carriage services to the public. In many cases IoT communications will pass over public networks (for example a fixed or cellular network operated by a mobile carrier).

However, experience suggests that over time, IoT operators (government is a possible example in relation to smart cities) may start to deploy their own network units and effectively vertically integrate both carriage and content services. In this case, the operator will become subject to the carrier licensing regime. Alternatively, technology aggregators may bundle and resell carriage services from third party networks to IoT providers, making these aggregators carriage service providers.

IP ADDRESSING ISSUES

There are currently two types of IP addresses in active use: IP version 4 and IP version 6. IPv4 was deployed in 1983 and is still the most commonly used version.[10] Given the numeric basis for IP addresses, Asia, Europe and the US have effectively run out of IPv4 addresses.[11]

IPv6 which has been available since the 1990s caters for trillions of IP addresses and offers more efficient network management, better security and interoperability for mobile networks. However many organisations have been slow in upgrading their hardware for the new version, which creates the risk of disruption as IPv4 addresses become oversubscribed. .[12]

[7] Jerome, Joseph, Big Data: Catalyst for a Privacy Conversation, 48 Ind. L. Rev. 213 2014-2015.

[8] CommsWire No. 150701, 1 July 2015.

[9] http://openinterconnect.org/

There is technical debate about whether IPv6 is an essential precondition to the widespread adoption of the IoT, as some IoT communication models can work within the limitations of the IPv4 model. A plausible outcome would seem to be a progressive migration to IPv6 over time in line with demand for IP identifiers.

ROAMING

Roaming is an inherent issue associated with the IoT since the vast majority of devices and sensors will be mobile and will therefore cross over network boundaries. Domestic roaming is currently not regulated in Australia but governed by inter-carrier agreements. While we do not advocate regulatory intervention in the emerging roaming services market for the IoT, an effective inter-carrier fee structure will be a precursor to the growth of the IoT.

By way of context, the ACCC last looked at whether it should declare mobile domestic inter-carrier roaming services in December 2004.[13] Relevant to its conclusion that it was premature to declare the service was the view that the competition in the market for retail mobile services was not yet fully effective and that there were geographic barriers to achieving nationwide coverage (e.g. availability of spectrum, economies of scale and sunk costs).[14] Similar considerations would seem to apply to IoT related roaming given the early stage of this technology's development.

SPECTRUM ALLOCATION POLICY

Often IoT devices transmit data using a local access technology such as bluetooth or wi-fi. This traffic then transits onto a fixed or, often, a mobile cellular network.

Since there is no national network engineered for low powered devices (such as IoT devices), the increasing amount of traffic already passing through these networks (especially wireless) combined with the likely surge in demand from the IoT adds further demand to the ever increasing need for more mobile bandwidth.

This is a knotty issue. In its recent Five Year Spectrum Outlook 2015-19, the ACMA has said "with the continuing emergence of technologies that rely on the use of spectrum for purposes such as machine-to-machine communications, the Internet of Things (IoT) and digital communications, demand for spectrum continues to grow."[15]

This means not only another demand pressure on mobile carriers for licensed (exclusive use) spectrum, but also creates a policy dilemma in relation to unlicensed (or "class licensed") spectrum which is typically used for local access wireless networks. There is only a limited amount of "class licensed" spectrum for listed purposes including the ISM band. However, some IoT operators are finding that free "class licensed" spectrum is becoming increasingly cluttered to the point where it is not fit-for-use for their devices, while licensed spectrum is prohibitively expensive.

Thus, for the IoT to be allowed to grow, the ISM band must be sufficiently large and fit-for-purpose to cater for the large number of devices that are likely to use the IoT. This raises important issues about the amount and type of ISM band spectrum which should be allocated for this purpose, and how this should be divided (if at all) between government (and government agencies) and business. In response to the Australian government's "Spectrum Review" (March 2015),[16] the ACMA has recently announced it will adopt the recommendations from the Spectrum Review and is presently considering ways to implement that Review including by creating a more flexible framework for spectrum access to balance the diversity and increasing number of uses and users.[17]

At the same time and in common with its counterparts in the US and Europe, one of the options the ACMA has been reviewing is the concept of spectrum sharing. This could mean that wireless carriers would share spectrum with the federal government or spectrum would be shared on a geographic basis for machine-to-machine technology.

A plausible outcome would seem to be a progressive migration to IPv6 over time in line with demand for IP identifiers

Overall it seems what is required is a mix of spectrum solutions, involving the appropriate mix of access to both licensed and open spectrum.

A LOW POWER WIDE AREA NETWORK FOR AUSTRALIA?

There may in the future be some IoT devices whose social utility justifies installation of dedicated network units to ensure uninterrupted communications. Some examples of this include smart city technology generally, priority assistance services, medical, defence or security applications.

This raises the spectrum issues mentioned above and a policy question for government

>

[10] https://www.iana.org/numbers

[11] http://au.pcmag.com/internet-products/30648/news/us-to-run-out-of-ipv4-addresses-this-summer

[12] http://www.pcmag.com/article2/0,2817,2376887,00.asp

[13] http://www.accc.gov.au/system/files/Final%20report%E2%80%94mobile%20domestic%20inter-carrier%20roaming%20service.pdf

[14] http://www.accc.gov.au/system/files/Final%20report%E2%80%94mobile%20domestic%20inter-carrier%20roaming%20service.pdf, paragraph 4.5.

[15] http://acma.gov.au/~/media/Spectrum%20Transformation%20and%20Government/Issue%20for%20comment/pdf/FYSO%202015-19%20pdf.pdf section 3.3 at page 23.

[16] file:///C:/Users/ausjh2/Downloads/Spectrum-Review-report-FINAL_-_for_publishing%20(1).pdf

[17] http://www.acma.gov.au/Industry/Spectrum/Spectrum-planning/About-spectrum-planning/acma-welcomes-spectrum-review-recommendations

about the extent to which it should be involved in deployment of such networks. For example, the UK Government chief scientific advisor (Sir Mark Walport) has made a number of policy recommendations in relation to the IoT, including that the UK government investigate whether a stable, low power wide area network be deployed to support existing fibre infrastructure.[18] Some governments have also embraced the concept of the smart city - for example, there are initiatives underway in India, Singapore and China.

It is possible then that the IoT discussion may evolve into a broader debate about whether there should be dedicated IoT networks as this technology matures and develops. This would be certain to raise similar issues around the current NBN debate such as cost, deployment, structure and policy framework (including competition issues).

an effective inter-carrier fee structure will be a precursor to the growth of the IoT

NET NEUTRALITY

As the IoT develops and involves increasing amounts of data, networks risk becoming congested. This raises the question of whether some data flows should be prioritised over others. For example, should data associated with health monitoring devices such as heart rate monitors or glucose readings should take priority over data flows updating a user's calorie intake.

The Internet is broadly based on the principle of net neutrality which requires there be an open Internet that allows users to go where they want, when they want. In support of this principle, in February 2015, the US Federal Communications Commission (**FCC**) adopted a set of Open Internet rules which seek to protect and maintain open, uninhibited access to legal, online content and prohibit ISPs from being allowed to block, impair or establish fast/slow lanes to lawful content.[19]

There is no equivalent rule in Australia, although there is a telecommunications interconnection access regime for declared services which is administered by the ACCC. This regime aims to facilitate third party access to certain services to promote the economically efficient operation and use of investment in infrastructure, and promote the effective competition in upstream and downstream markets. The declared services regime does not currently impose net neutrality rules on Australian carriers.

In contrast, the US FCC Open Internet rules apply to both fixed and mobile broadband services and involve three key principles:

1. no blocking - ISPs must not block access to legal content, applications, services or non-harmful devices;
2. no throttling - ISPs must not impair or degrade lawful internet traffic on the basis of content, applications, services or non-harmful devices; and
3. no paid prioritisation - ISPs must not favour some lawful internet traffic over other lawful traffic in exchange for consideration of any kind (including from their affiliates).

The FCC has taken the position that bandwidth services are considered utilities (like water and gas) and therefore subject to considerable regulatory restrictions. These restrictions prevent ISPs from requesting additional fees for faster connection services or for blocking some types of content. Complaints for overcharging are investigated by the FCC.

The Open Internet rules do not yet have any specific IoT parameters. So it is uncertain how they would apply to situations where there may be a legitimate reason to prioritise certain enterprise traffic over others e.g. health monitoring applications or public safety applications or to de-prioritise certain non-essential services when traffic is congested.

CONCLUSIONS

This short overview has shown the many issues emerging from the IoT. Governments around the world have been somewhat active in addressing these issues. For example, the European Union considers the IoT an essential part of its Digital Agenda for Europe 2020; other sovereign initiatives are described above.

To some extent in Australia the legal and policy response to the IoT continues to be a work in progress. The response is informed by the international developments mentioned above as well as the unique challenges of the Australian communications environment. What is clear is that the IoT presents a range of complex and inter-related policy issues which will become only more pronounced as this technology matures.

In part two to be published in the final edition of the CAMLA Bulletin of 2015 we will consider issues arising out of the IoT that are unique for government and consumers.

JAMES HALLIDAY is a partner and REBEKAH LAW is an associate in the corporate group at Baker McKenzie in Sydney.

This article represents the personal view of the authors and is not necessarily representative of the views of any client of the firm.

[18] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/409774/14-1230-internet-of-things-review.pdf ; recommendation 4a.

[19] https://www.fcc.gov/openinternet