Australian Government

acma

Australian Communications and Media Authority

researchacma
Evidence that informs

The Internet of Things and the ACMA's areas of focus

Emerging issues in media and communications Occasional paper

NOVEMBER 2015

communicating
facilitating
regulating

Canberra
Red Building
Benjamin Offices
Chan Street
Belconnen ACT

PO Box 78
Belconnen ACT 2616

T +61 2 6219 5555
F +61 2 6219 5353

Melbourne
Level 32
Melbourne Central Tower
360 Elizabeth Street
Melbourne VIC

PO Box 13112
Law Courts
Melbourne VIC 8010

T +61 3 9963 6800
F +61 3 9963 6899

Sydney
Level 5
The Bay Centre
65 Pirrama Road
Pyrmont NSW

PO Box Q500
Queen Victoria Building
NSW 1230

T +61 2 9334 7700 or 1800 226 667
F +61 2 9334 7799

Contents

Executive summary

The Internet of Things (IoT) refers to the inter-connection of many devices and objects utilising internet protocols, and it is yet another phase in the convergence of communications and its role as a fundamental enabler within the wider economy.

While there are many different projections about the likely number of connected devices in Australia, there is a growing industry consensus that IoT will be characterised by a rapid increase in the number of connected devices and a rapid evolution in the range of associated applications and services on offer as a consequence.

Significant productivity benefits are also expected to be realised, with a recent McKinsey & Company report estimating a potential global economic impact of IoT applications of $11.1 trillion (USD) per year in 2025.[1]

Australia is well placed to realise a share of these potential productivity gains, with the Australian communications and digital information industries demonstrating significant capacity over many years in leading and responding to change. Australian consumers and citizens have also shown a similar appetite for embracing new forms of communications technology and adapting their communications practices.

As the regulator for communications and media, the Australian Communications and Media Authority (the ACMA) is assessing how existing regulation can be used to facilitate and enable Australian businesses and citizens to benefit from IoT innovations. To date, the ACMA has responded to requests by industry participants seeking clarification about spectrum availability to support IoT applications. This has prompted the ACMA to therefore consider more broadly the other aspects of its regulatory remit that may be used to facilitate IoT developments in Australia.

In this paper, the ACMA has focused on aspects of its regulatory remit that support the following enablers of the IoT:

- **infrastructure connectivity**, using telephone numbers and spectrum
- **devices**, including device standards
- **digital data** and **information**
- the **capabilities** of Australian businesses, consumers and citizens to manage multiple devices, connections and information.

The analysis looks at the likely sources of regulatory pressure that will arise in an environment characterised by multiple and complex connections of devices, such as machine-to-machine (M2M) connections as well as the connection of digital information. It examines the existing regulatory settings and underpinnings of regulatory concepts that have an ongoing utility in supporting the complex connections of an IoT environment.

[1] McKinsey Global Institute, *The Internet of Things: Mapping the Value Beyond the Hype*, June 2015, p. 2.

This paper also identifies some priority areas for regulatory attention that will be important in facilitating IoT developments in the near, medium and longer term. These suggested priority areas include:

- resource allocation such as spectrum and telephone numbers needed for communications infrastructure
- managing network security and integrity
- supporting the interoperability of devices and information through standards-setting
- supporting Australian business, citizens and consumers to develop stronger digital technical capabilities and literacy to interact constructively with devices and mediate their way through the increasing complexity of digital information.

This initial analysis also indicates that the balance of regulatory interventions in the future is likely to skew more towards the enabling strategies of facilitation and communication—strategies that aim to encourage innovation and the adoption of IoT applications.

Feedback—tell us what you think

In this paper, the ACMA is looking at Australia's state of readiness for a transition to the IoT and asking is there more that needs to be done by industry, citizens and by the regulator to facilitate the development of the IoT in Australia?

The ACMA welcomes comments and feedback in response to:

1. The ACMA would welcome any proposals from industry around the need for the designation of a discrete numbering range for M2M or IoT applications.
2. The ACMA would welcome views from industry about future spectrum requirements to support M2M and IoT applications.
3. The ACMA would welcome input from industry as to how cooperative models of information sharing and action by industry, citizens and regulators might be adapted to address newer forms of digital information harms.
4. Are there any additional issues that should be included as priorities for the regulator's attention that have not yet been identified in this paper?
5. Has the ACMA correctly identified the near-, medium- and longer-term priorities for attention by the regulator?

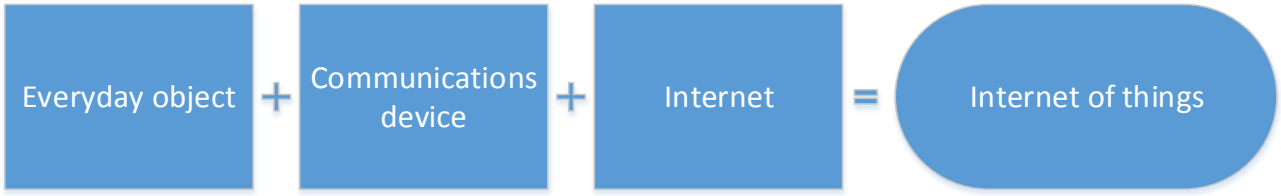
How to provide feedback

- **By email**—please email research.analysis@acma.gov.au.
- **Online**—use our new beta online consultation facility to provide comments and answers to the questions above.

About the research

The Internet of Things (IoT) refers to the inter-connection of many devices and objects utilising internet protocols that can occur with or without the active involvement of individuals using the devices. The IoT is the aggregation of many machine-to-machine (M2M) connections (see Figure 1).

Figure 1: M2M and the IoT



Source: ACMA Five-year spectrum outlook 2015–19.

A more expansive definition encompasses the Internet of Everything (IoE), which reflects that the IoT is not limited to communications, but includes big data analysis, cloud computing, and sensors and actuators that, in combination, can efficiently run autonomous machines and intelligent systems.[2]

As the communications and media regulator, the ACMA has documented over time the impact of convergence pressures on the communications and media sectors. In this occasional paper, the ACMA:

- identifies how the ACMA will facilitate M2M and IoT innovations within the scope of its existing regulatory remit over the next five to 10 years
- provides additional supporting analysis examining a range of issues in Australia's transition to M2M communications and the IoT
- undertakes an initial review of existing regulatory settings to identify relevant regulatory tools and strategies that might better facilitate M2M and IoT.

research**acma**

Our research program—research**acma—**underpins the ACMA's work and decisions as an evidence-informed regulator. It contributes to the ACMA's strategic policy development, regulatory reviews and investigations, and helps staff better understand the agency's role in fulfilling its strategic intent to make media and communications work for all Australians.

research**acma** has five broad areas of interest:

- market developments
- media content and culture
- social and economic participation
- citizen and consumer safeguards
- regulatory best practice and development.

This research contributes to the ACMA's market developments and regulatory best practice and development research themes, reflecting the importance of IoT as an

[2] OECD, Committee on Digital Economy Policy, Digital Economy Outlook, Chapter 5 Emerging Issues; The Internet of Things, p. 4.

enabling technology development. Consequently, this paper offers some insights into how future regulatory arrangements could be designed to further facilitate IoT applications.

This paper continues the ACMA's recent focus on emerging issues in media and communications. Past papers in this series include:

- *Mobile apps—Emerging issues in media and communications, occasional paper 1* (May 2013)
- *Near-field communications—Emerging issues in media and communications, occasional paper 2* (May 2013)
- *The cloud: services, computing and digital data—Emerging issues in media and communications, occasional paper 3* (June 2013)
- *Privacy and personal data—Emerging issues in media and communications, occasional paper 4* (June 2013)
- *Six emerging trends in media & communications* (November 2014).

A forthcoming paper in the *Emerging issues* series will examine 5G mobile technology developments.

Introduction

Over the past 10 years, communications and media in Australia has undergone a period of massive innovation, with accompanying disruption to existing business models and industry structures. These changes have been documented by the ACMA's tracking studies of market and technology developments and longitudinal studies of Australian's changing media and communications practices.[3]

The Pew Research Center (as part of a sustained effort throughout 2014 to mark the 25th anniversary of the creation of the World Wide Web) examined the future of the internet, the web, and other digital activities. They canvassed 2,558 experts and technology builders about where we will stand by the year 2025 and found striking patterns in their predictions.[4] To a notable extent, these experts agreed on the technology change that lies ahead, even though they disagree about its ramifications. Most believe there will be:

- 'augmented reality' enhancements to real world displays that people perceive through the use of portable/wearable/implantable technologies
- disruption of business models established in the 20th century (most notably impacting finance, entertainment, publishers of all sorts, and education)
- tagging, databasing, and intelligent analytical mapping of the physical and social realms
- a global, immersive, invisible, ambient networked computing environment built through the continued proliferation of smart sensors, cameras, software, databases, and massive data centers in a world-spanning information fabric known as the 'Internet of Things' (IoT).

The IoT and other developments such as those chronicled above by Pew Research are unleashing what is often discussed as 'forces of disruption'. Catherine Livingstone, Chair of Telstra, Australia's major telecommunications company, put it this way in a recent address:

> At the heart of this disruption is connectivity. Mass connectivity.
>
> This connectivity has enabled human generated data, and now machine generated data, to flood through our global networks of fibre and copper. Combined with orders of magnitude increases in computing power, what and who is possible to know is almost limitless. And in real time.
>
> We thought that the connectivity enabled in the mid-nineties by the fixed line Internet and browser technology was disruptive; that was before 2007, when the mobile internet became a reality with the first smartphone. But that is nothing compared with the disruption we will see with the advent of the 'internet of things.'[5]

There are a number of other ingredients feeding into the mix headlined by the IoT—cloud computing, 'deep learning' algorithms fed by big data, the smart devices in the hands of consumers and citizens, and the connectivity platforms that support disruptive business models currently challenging many established industries.

---

[3] ACMA, *Evidence informed regulatory practice: an adaptive response, 2005–15*.

[4] Pew Research Center, Digital Life in 2015.

[5] Catherine Livingstone, President Business Council of Australia, National Press Club address, 29 April 2015.

The growing reach of the IoT and the emerging Internet of Everything (IoE) is likely to involve a step-change not only for industry and innovation, but is also equally likely to drive significant behavioural changes in the way Australians interact with each other, with machines, and with networked digital information. Many of the building blocks to support mass connectivity are in place. However, the ACMA's observation is that industry segments and sectors, along with individual consumers and citizens, are at different stages in transitioning towards that densely connected world of an internet-enabled everything.

Identifying where there are barriers to innovation, or where confidence in undertaking new activities needs bolstering, will be important in ensuring that Australia derives maximum benefit in a hyper-connected environment.

The capacity of the Australian communications industry sector to address these barriers has direct consequences for Australia's economic productivity and prosperity.

According to the recent Australian Infrastructure Audit, the direct economic contribution of communications services across Australia was $21 billion in 2011—the highest contribution of any of the infrastructure sectors. Growth projections estimate that the direct economic contribution of communications is expected to grow to approximately $42 billion by 2031.[6] This estimate only covers communications and does not take account of the contribution of digital content and media. Nor does this estimate model the non-linear effects that occur from major disruptive technology, market or social changes.

Australian communications and content industries have demonstrated significant capacity over many years in leading and responding to change. Australian citizens and consumers have also shown a similar appetite to embrace new technologies and communications practices.

However, the cautionary note struck in these industry commentators' observations highlights the importance of having in place the appropriate regulatory settings that will enable M2M and IoT developments to flourish, as well as mitigate any potential harms. This point is noted in the report from The McKinsey Global Institute (MGI) in its comprehensive assessment *The Internet of Things: Mapping the Value Beyond the Hype,* which examines the impact of IoT across nine environments: homes, offices, factories, worksites (mining, oil and gas, and construction), retail environments, cities, vehicles, and the outdoors. MGI noted that:

> … policy makers and governments will have to ensure that these new systems are safe and that IoT data is not being stolen or abused. They can help to balance the needs for privacy and protection of private data and intellectual property with the demands of national security. With vital infrastructure connected to the Internet, security threats will multiply, which governments will need to address. Policy makers also have an important role in enabling the Internet of Things by leading and encouraging standards that will make interoperability and widespread adoption possible.[7]

As one of the relevant regulators in the Australian context, the ACMA can work with industry to better resolve impediments to the development of IoT by explicitly forbearing on regulation or by the use of targeted regulatory interventions.

[6] Infrastructure Australia, Australian Infrastructure Audit, May 2015.

[7] McKinsey Global Institute, *The Internet of Things: Mapping the Value Beyond the Hype*, June 2015, p. 125

Accordingly, in the first part of this paper, the ACMA has developed an IoT roadmap to chart a practical course in the context of its existing legislative remit to engage with this aspect of communications innovation.

In the second part of the paper, the ACMA provides additional analysis supporting the prioritisation of the areas identified in the roadmap for attention and facilitation by the regulator, and the third part of the paper provides further guidance on the ACMA's framework for regulatory analysis.

Part 1—A practical roadmap

This part looks at the practical responses under development by the ACMA in the context of its existing legislative remit. This analysis is primarily concerned with identifying where and when the ACMA can act to assist industry and consumers in the development and adoption of IoT applications.

The ACMA's current focus

The ACMA's current focus, as outlined in its Corporate plan, is directed towards facilitative actions to establish the conditions and settings that will support M2M and IoT developments, as well as identify potential inhibitors to those developments.[8] The ACMA has examined the regulatory settings of the different enabling aspects of M2M and IoT through its previous work looking at short-range mobile network applications such as near-field communications, big data and cloud computing. As part of its ongoing resource planning activities, the ACMA has also looked at the immediate industry requirements for access to spectrum and telephone number resources. The ACMA is engaged in discussion with industry stakeholders about reviewing existing regulatory settings to identify regulatory tools and strategies that will further facilitate M2M and IoT applications.

Telephone numbers as an infrastructure enabler

As an area of immediate focus, the ACMA is continuing to cater for growth in M2M and IoT applications by making telephone numbers and spectrum available.

M2M reliance on mobile networks is expected to continue in the short term, reflecting the easy availability of mobile network technologies. In the context of its Numbering Work Program, the ACMA considered the effect of M2M on the demand for mobile numbers. At the time (2011), the early estimates suggested a requirement for numbers for M2M communications of between 5.8 and 61.9 million by 2020.[9] In responding to this expected demand for new mobile numbers, in 2012 the ACMA made available a new mobile number range (05 range) to supplement the existing (04) mobile number range. The ACMA will continue to monitor changes in demand for mobile numbers used in M2M communications.

Invitation to comment:

1. The ACMA would welcome any proposals from industry around the need for the designation of a discrete numbering range for M2M or IoT.

Spectrum as an infrastructure and device enabler for IoT

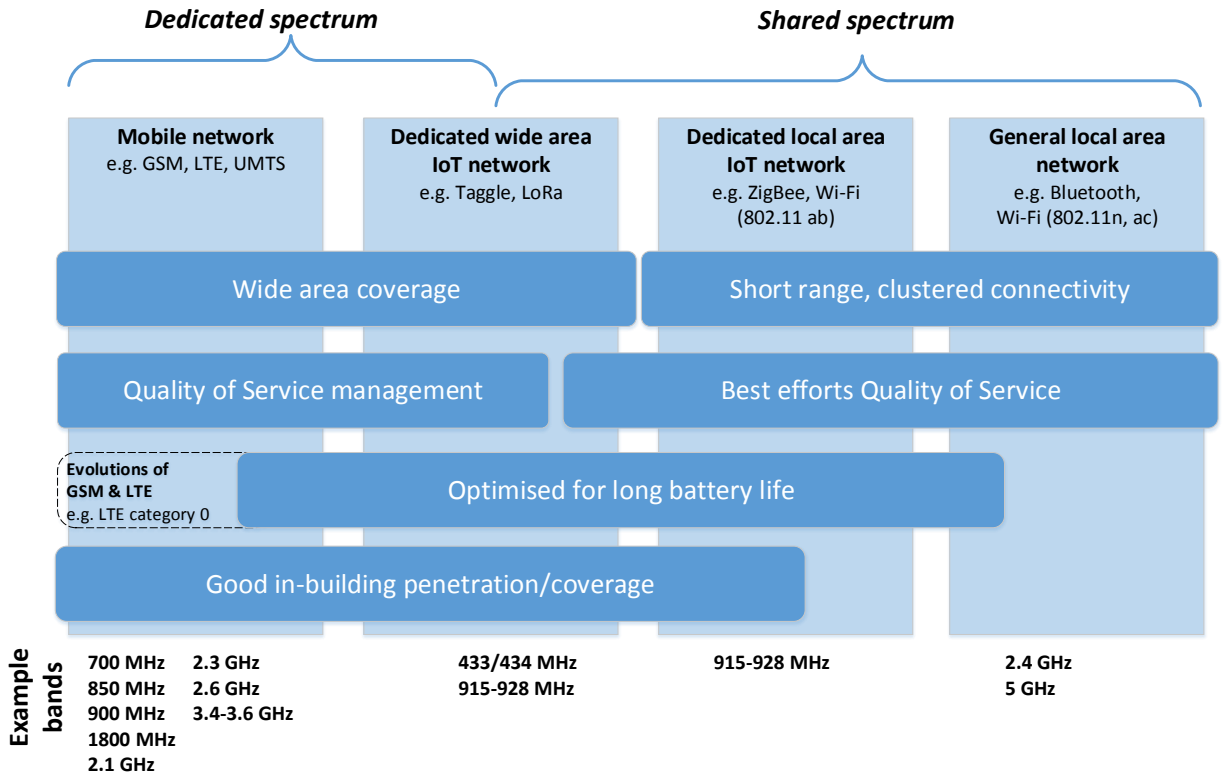
Similarly, the immediate focus in spectrum planning is concerned with accommodating M2M and IoT applications within the existing licensing framework and the identification of candidate spectrum bands to address expected future demand. This spectrum planning approach is outlined in the ACMA's Five-year spectrum outlook.

[8] ACMA, Corporate Plan 2015-19, p. 5.

[9] ACMA, *Numbering: Structure of Australia's telephone numbering plan—Consultation paper number one*, p. 48.

When it comes to the designation of particular spectrum bands to support M2M and IoT applications, a mix of licensing arrangements and variety of spectrum bands may be required to support different IoT use cases (see Figure 2).

Figure 2: Spectrum identified for IoT applications



Source: ACMA, based on Ofcom model 2015, updated for Australian spectrum band plans.

The ACMA has licensing arrangements in place that encourage innovation in M2M and IoT via the class-licensing regime. To some extent, M2M and IoT applications may utilise existing class licensed spectrum (that is, spectrum 'commons). Class licences authorise users of designated segments of spectrum to operate on a shared basis. A class licence is not issued to an individual user and does not incur licence fees. Unlike other forms of spectrum licensing (namely, apparatus and spectrum licences) that are issued and used on an individual basis, use of this type of 'unlicensed' spectrum does, however, come with the cost of a higher likelihood of interference.

Currently, spectrum that is globally available at a low cost (or free as class licensed spectrum) is in the Industrial Scientific Medical (ISM) bands, which include the 900 MHz band, the 2.4 GHz band and the 5.6 GHz band.

In relation to other specific spectrum bands under review during 2015–16:

- the scheduled review of the 803–960 MHz band will explore future opportunities as a candidate band for mobile broadband and M2M
- the review of the 5.9 GHz band for intelligent transport systems applications is also relevant as intelligent transport systems represent one of many IoT applications.

Invitation to comment:

2. The ACMA would welcome views from industry about future spectrum requirements to support M2M and IoT applications.

Enabling seamless information exchange for digital data

In other jurisdictions, the ACMA is observing strong interest in the network and information security and reliability issues that arise in the IoT environment in the connections between people, devices and data.

The need for seamless information and data exchange, between machines and machines, and people and machines, may be facilitated by industry development of protocols for managing data portability and interoperability standards dealing with information exchange.

The other element of providing confidence in regulatory settings to further enable IoT requires a mechanism to address concerns with information security risks. There are existing models in use that may provide some design insights where additional interventions are required.

Currently, some internet security risk concerns are addressed via the Australian Internet Security Initiative (AISI), which is a co-operative program between the ACMA, internet service providers and citizens. The AISI was developed with the objective of protecting Australian internet users from malware (malicious software).and cybersecurity threats on the internet.

This program model relies on information-sharing and action by industry, citizens and the regulator. The ACMA collects infection data from a variety of sources and feeds this into the AISI. Daily infection reports are then provided to participating Australian internet providers, that include internet service providers (ISPs) and other organisations such as universities that have been allocated IP (internet protocol) ranges and manage their own networks. These reports identify IP addresses that have been infected in the previous 24-hour period. Internet providers correlate their customer data with the IP address information provided through the AISI to determine the customers associated with the infection, and then inform them of the infection. Internet providers are also expected to advise their customers on how to remove the infection and help prevent future infections from occurring. This not only helps protect the internet user from the consequences of the infection, but also prevents the infected computer from undertaking further malicious activities on the internet. The AISI has been strongly supported by Australian internet providers, with 124 ISPs and 18 educational institutions currently participating—representing well over 95 per cent of Australian residential internet users.

This co-operative model may provide useful insights as a way to address other forms of networked harms that may arise in the IoT environment.

Invitation to comment:

3. The ACMA would welcome input from industry as to how cooperative models of information sharing and action by industry, citizens and regulators might be adapted to address newer forms of digital information harms.

Developing citizen's and consumer's digital capabilities

The ACMA is also directing its attention to monitoring marketplace changes so that there is an evidence base available to inform industry and policy makers about the speed of changes occurring in the market and in citizen and consumer communications behaviours.

The available evidence indicates an increased fragmentation of audience and consumer behaviours, which pose particular challenges for the future when regulatory design is often based upon uniform regulatory solutions.

Despite increasing levels of digital engagement and increasing complexity in the number of devices and connections made, over one million Australians (around six per cent) have never accessed the internet. This group of unconnected Australians, while reducing over time, poses a significant challenge for how Australia will manage the transition to IoT, where there are very different levels of experience, skills and confidence in using communications technologies across the community.

For connected Australians, there may be additional challenges in fully utilising IoT connections due to network access issues, managing device compatibility issues or having the skills to undertake the necessary software upgrades to manage network and device connections.

There is an opportunity in this innovative environment to also focus on the development of the necessary skills and confidence of citizens and consumers so that they can operate productively in shaping their connections and information exchange for IoT applications.

Invitation to comment:

4. Are there any additional issues that should be included as priorities for regulatory attention that have not yet been identified in this paper?

The ACMA's medium-term focus—the next two to five years

Over the next two to five years, progress in the take-up and use of M2M applications and the transition to IoT will give more clarity on the demand for resources and the overall capability of business and citizens in using IoT applications. Facilitating and enabling the use of M2M and IoT is expected to remain an important focus for the ACMA.

In relation to telephone numbers, it is likely that M2M communications will broaden from current technologies reliant on mobile numbers, to be supplemented by IP-based communications using IP addresses (IPv6), as mobile broadband and next generation network fixed technologies become ubiquitous in this period.

Spectrum band planning will continue to review bands that will support M2M and IoT applications, within the time frames and band planning outlined in the Five-year spectrum outlook.

In this time frame, work in international forums (such as the ITU-R World Radiocommunication Conference 2018/19) will be important in considering future spectrum needs for a broad range of services. Some of these may accommodate IoT applications, in particular the consideration of spectrum for IMT above 6 GHz and for intelligent transport systems.

Planning processes for the international standardisation of 5G technologies that will support the 'anytime, anywhere, anyone and anything' capability needed for the IoT will continue through this period.

Tracking the take-up and use of IoT applications, and identifying where there are emerging areas of concern by business or the community, will inform whether there is a need for any further action.

One of the key reasons to measure the speed and scale of change occurring in Australian communications is to assess whether existing regulatory settings inhibit or facilitate the new developments occurring and Australia's adoption of IoT applications.

The ACMA's longer-term focus—five+ years

Beyond a five-year time frame, if forecasts of the number of connected devices come to fruition, then Australia can expect a very different communications environment.

However, the key components needed to make IoT work remain relevant and offer a basis to inform where industry, citizens and regulators may need to invest attention.

Communications infrastructure planning has tended historically to occur over long (10 to 15 years+) time frames, reflecting the need for international harmonisation of technology and device standards that then informs demand and the identification of particular spectrum bands for release for IoT applications. Even if the expected planning cycle truncates further in future, elements of the design standards specification and international harmonisation of spectrum bands remain important components in providing a more certain investment environment IoT applications.

With the autonomous machines of M2M and IoT, there is a heightened awareness of the importance of the integrity of network security and reliability, along with device and information security. With information and digital data being another key enabler of IoT, information standards, including protocols related to personal information and information portability, are likely to become more important to effective IoT applications.

Finally, the capabilities of Australian businesses and consumers to manage their networks, devices and information with confidence and security will be crucial to Australia's capacity to garner the productivity benefits of IoT.

The role that regulatory settings play in contributing to confidence and enabling the development of innovative IoT applications will inevitably involve a reassessment of the relevant supporting policy objectives and whether they can continue to be met by lessening, or extending regulation, or applying the existing suite of regulatory tools and interventions in a different way.

Invitation to comment:

5. Has the ACMA correctly identified the near, medium- and longer-term priorities for regulatory attention?

Part 2—Enabling the Internet of Things

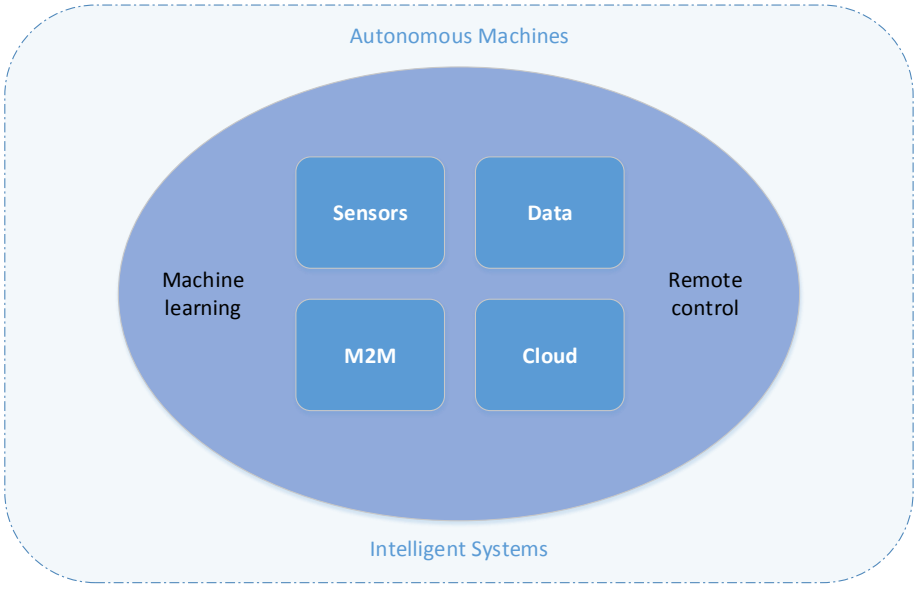
This second part of the paper looks in more detail at the areas of activity that are expected to enable M2M and IoT applications.

It examines relevant and existing regulatory strategies and tools can be used to support these technology and industry developments.

Enablers of the Internet of Things

According to the Organisation for Economic Co-operation and Development (OECD), the main enablers of IoT include sensors that provide an interface between the physical world and a device, big data, M2M and cloud computing (Figure 3).

Figure 3: Main enablers of the IoT



Source: OECD Digital Economy Outlook Chapter 5: Emerging Issues: The Internet of Things, p. 8.

Many of these enabling elements feature in Australians' current communications practices, with the ACMA having considered the implications for regulation of a number of these developments.[10]

Examples of existing and potential M2M applications include:

- vending machines and parking meters (to signal that a particular product is depleted or the machine requires service)
- monitoring of smart meters by electricity, gas and water utilities

[10] ACMA, *Near-field communications—Emerging issues in media and communications, occasional paper 2*, (May 2013), *The cloud: services, computing and digital data—Emerging issues in media and communications, occasional paper 3* (June 2013).

- automatic notification by vehicles to emergency service organisations of serious road accidents[11]
- tracking of assets such as fleet vehicles, trucks, ships, trailers, containers and expensive medical equipment
- security alarms
- supervision and surveillance systems.

Taken together, these separate developments form part of Australia's ongoing transition towards increasingly complex connections—enabled initially by the digitalisation of networks and content, being accelerated through M2M communications and expanding exponentially under the IoT.

The OECD noted that the pace of developments in the IoT may be much faster than that of the mobile phone services over the past two decades, with suggestions that:

> The number of connected devices in a house in OECD countries is expected to be 14 billion by 2022—up from around 1.4 billion in 2012.[12]

On a global scale, Gartner's most recent prediction suggests 6.4 billion connected things in use worldwide in 2016, with an estimated rate of 5.5 million new device connections occurring every day.[13]

Even the most conservative assessments indicate a rapid increase in the number of connections and rapid evolution of IoT applications and services on offer.

While Australia has many important building blocks in place to support increased connectivity, it remains unclear how the expected exponential increase in connections between humans and machines, and then connections without human interaction, will alter economic and social structures and practices.

Enabling infrastructure

Network digitalisation and increasingly higher bandwidth

Engaging in the IoT is premised on access to IP-enabled wired and wireless networks that are capable of exchanging and storing large amounts of information.

Since the 1980s, Australia has undergone a significant transformation at the network infrastructure layer with the digitalisation of telecommunications and broadcasting networks. Broadcasting digitalisation was completed as recently as 2013. Digitalisation of fixed-line telecommunications networks commenced in the 1980s but has had a longer maturation path, with the upgrade of the last mile a work in progress as the National Broadband Network (nbn) is rolled out.

Australia has benefited from the progressive addition of mobile broadband capacity, first with 2G networks, through to the current ongoing rollout of 4G networks. Theoretical planning for 5G spectrum capabilities is already underway internationally and in Australia, noting that the 'anytime, anywhere, anyone and anything' capability of 5G will be critical to underpin increased M2M and IoT capabilities in Australia.

---

[11] See September 2009 European Commission announcement, 'European Commission urges EU countries to implement eCall voluntarily', at www.epractice.eu/en/news/293342.

[12] OECD, Committee on Digital Economy Policy, Digital Economy Outlook, Chapter 5 Emerging Issues; The Internet of Things, p. 19.

[13] Gartner, Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015

However, it is still too early to characterise where the next improvements will occur in the still-evolving definition of 5G technologies. There is significant ongoing research into improvements in wireless technology, but there is no industry consensus yet on how 5G technologies will support IoT.

Some industry participants regard the next wireless technology developments as 'evolutionary' improvements to the existing wireless parameters, providing improved coverage, reliability and network density.

Other industry participants consider that improved data rates and the lower latency of 5G will provide a 'revolutionary' leap forward that will support ubiquitous IoT. This includes the capacity to support many connected devices under M2M, increased data storage for cloud computing, and anywhere and anytime connections needed for connected cars, all of which are considered by some to be unachievable using current wireless generation technologies.

Addressing and numbering

Network addressing that connects devices currently relies on telephone numbers (for devices connected via cellular telephony networks) or internet addresses.

While estimates of the growth of M2M communications vary significantly, Cisco's Visual Networking Index estimated some 115.7 million connected devices in Australia in 2014, which is forecast to rise in five years to 219 million.[14]

In Australia, the telephone numbering resource is managed by the ACMA. Digital mobile numbers are used in connection with M2M communications. Based on current demand forecasts, the ACMA estimates there is approximately seven years' supply in the (04) digital mobile number range. In 2012, the ACMA specified additional capacity—the 05[15] number range—to cater for anticipated demand for digital mobile numbers. Specification of the 05 number range provides an additional 99 million numbers that can be used in connection with digital mobile services including M2M.

In the short term, while there are not expected to be immediate concerns with the number supply, the ACMA will need to continue to monitor demand for digital mobile numbers as M2M and IoT applications develop.

Internet addressing schemes are also used for M2M and IoT communications. In Australia, the internet addressing registry is managed by the Asia–Pacific Network Information Centre (APNIC) with global coordination undertaken by the Internet Corporation for Assigned Names and Numbers (ICANN), in accordance with guidelines made by the Internet Engineering Taskforce.[16] Australia, consistent with global practice, is transitioning from internet protocol version four (IPv4), which uses 32-bit addresses, to internet protocol version six (IPv6), which uses 128-bit addresses. IPv4 addresses are predicted to reach exhaustion in the near term. IPv6 addresses offer a number of advantages over IPv4 addresses, including enhanced security.

---

[14] Cisco Visual Networking Index Forecast Highlights

[15] With the exception of the prefix 0550, which is specified for use in connection with the supply of location independent communications services.

[16] See RFC 2050, *Internet Registry IP Allocation Guidelines*, first published in 1996; RFC 2928, *Initial IPv6 Sub-TLA ID Assignments*, first published in September 2000; RFC 3177, *IAB/IESG Recommendations on IPv6 Address Allocations to Sites*, first published in September 2001. RFC refers to 'request for comment', and is the title used for internet standards documents and other publications of the Internet Engineering Taskforce.

It is unclear to the ACMA (and there is some debate internationally) when and if internet names and addresses and application-specific identifiers will replace telephone numbers for all M2M and IoT communications.

The ACMA has undertaken an extensive review of the administration of telephone numbering arrangements and examined the future direction of telephone numbers and the complementary role of internet addresses and identifiers.[17] In the short to medium term in Australia, the ACMA nonetheless considers that use of internet names and addresses and application-specific identifiers for a diverse array of communications services will grow, with telephone numbers remaining useful for niche deployments of IoT applications, but largely complementary to internet addressing.

Appropriate spectrum availability

In Australia, Cisco estimates that 35 per cent of all networked devices will be mobile-connected by 2019.[18] Industry and consumer demand for and use of devices and services on mobile networks are key drivers for increasing mobile traffic. Increases in mobile traffic and congestion can be responded to in several ways by mobile network owners, by adopting more spectrally efficient technologies, deploying additional network infrastructure or acquiring more spectrum.[19]

This may lead to demand for the designation of particular spectrum bands for particular types of IoT applications, such as intelligent transport systems, infrastructure and environmental monitoring, building automation.

However, the impact of traffic growth in M2M-like applications is somewhat more difficult to quantify. While it is likely that there may eventually be many more M2M connections than traditional mobile broadband type devices/connections, some of these connections will be for low data rate applications and can tolerate high latencies.

Therefore, many M2M connections may be able to operate in 'off peak' periods where demands on the mobile broadband network are low. Further, some M2M traffic will be carried over other networks (for example, low power, low duty cycle dedicated networks) rather than mobile broadband networks. In both cases, this may mean that the impact of network capacity demands from M2M will be less than for traditional mobile broadband connections.

Demand for devices to support M2M and IoT applications is nonetheless expected to increase pressure on industry operators to achieve low unit acquisition, implementation and operation cost for such devices. Globally harmonised standards are a key way to realise manufacturing economies of scale and allow a single IoT device type to be manufactured for multiple markets to achieve a lower unit cost per device.

Current developments of IoT focus on spectrum use where that spectrum is globally available currently at a low cost (or free). This is currently the Industrial Scientific Medical (ISM) bands.

ISM bands are to a large degree globally harmonised. In Australia, access to these bands is governed by the Radiocommunications (Low Interference Potential Device Class licence) 2000, known as the LIPD Class licence. The LIPD Class licence has

[17] ACMA, *Telephone numbering—Future directions*, November 2011, p. 9.

[18] Cisco Visual Networking Index Forecast Highlights

[19] Analysys Mason, Updated final report for the Australian Communications and Media Authority, *Mobile Network Infrastructure Forecasts*, June 2015, p. 15.

over 50 items that would permit M2M or IoT type operations, including for high latency, low power, low data rate devices requiring high reliability.

Other potential options for low power, low duty cycle devices are in the 900 MHz class licensed band, as well as the 2.4 GHz band and the 5.6 GHz band.

While IoT applications are expected to flourish in the existing spectrum commons, some industry operators are expected to seek greater certainty in their use of the spectrum through apparatus and spectrum licensing.

An immediate planning priority identified in the ACMA's Five-year spectrum outlook is the review of the 803–960 MHz band, which is examining current mobile broadband spectrum planning arrangements, in addition to the potential frequency arrangements for M2M communications.[20] The ACMA also continues to monitor international developments in intelligent transport systems (ITS) in the 5.9 GHz band, waiting for an opportune time to establish a regime in Australia that will build on a pre-existing trial.[21]

In planning for future spectrum needs, the ACMA continues to monitor international developments and is working within the ITU-R World Radiocommunication Conference planning processes for international harmonisation of 5G technologies that will support the 'anytime, anywhere, anyone and anything' capability needed for the IoT.

Increased device functionality

Connected devices are the lynchpin of the M2M and IoT environment, linking people and machines with each other and with information.

Currently, it is estimated that there are 14 billion IoT devices in use globally.[22] Forecast worldwide growth has varied considerably, with earlier Cisco[23] and Ericsson[24] estimates predicting that the number of networked devices would reach 50 billion by 2020. More recent predictions by Cisco, Ericsson and Gartner[25], estimate the growth of networked devices to reach 20 to 26 billion by 2020. In Australia in 2014, the figure was 115.7 million networked devices, which is expected to grow to 219.6 million networked devices within five years.

Each recent improvement made in network capacity has been accompanied by increased functionality across a range of devices. In the personal device market, the introduction of smartphones in Australia, followed by tablets, has seen progressive increases in the amount of information downloaded by Australians. Smartphone functionality brings the IoT closer to the individual consumer. Australians have significantly increased their use of portable internet devices (such as mobile phones and tablet computers), with the take-up of these devices increasing by three and four percentage points respectively in the 12-month period to May 2015.

Another feature of the mobility of devices and information is the rapidly-growing number of internet-accessible wearable devices that allow individuals to track their

---

[20] ACMA, *Five-year spectrum outlook 2015–19*, p. 50.

[21] ACMA, *Five-year spectrum outlook 2015–19*, p. 51.

[22] Cisco Visual Networking Index Forecast Highlights

[23] Dave Evans, CISCO, *The Internet of Things—How the Next Evolution of the Internet is Changing Everything*, April 2011, p. 3.

[24] Ericsson, CEO to Shareholders: 50 Billion Connections 2020, press release, April 13, 2010.

[25] 2014 Cisco Visual Networking Index; Gartner, Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015, November 2015; Ericsson Mobility Report, June 2015, p. 10.

activities. Real-time continuous information on a range of personal indicators can offer numerous benefits, including improved health monitoring and increased productivity.

As at May 2015, approximately half of all Australian homes had more than five devices connected to the internet via a home network.[26] Forecasts predict an increase in this figure to nearly nine networked devices per person by 2019.

As the number of terminal devices and services typically found in an Australian home today—personal and portable computers, tablets, smartphones, games consoles, security and home automation systems, connected appliances, central storage and backup systems—connect in the M2M and IoT environment, the complexity of Australians' connected home environment and the complexity of personal information exchanged and stored is expected to significantly increase.

Privacy, reliability and interoperability

There is already a growing interest in privacy and security management as smart devices generate increasing amounts of personal data. IoT applications are expected to dramatically increase the amount of information and data moving between machines and devices, and between individuals and devices.

As data and information becomes more highly networked, it elevates network reliability and security considerations as an important underpinning design element for IoT applications.

Some aspects of M2M and IoT will involve the machine-initiated exchange of digital data generated by or about individuals, particularly under person-to-person and machine-to-person connections.

While there are well-established privacy rules that govern the disclosure, collection and storage of personal information[27], a new challenge posed by IoT will centre on the management of notice and consent for communications that do not involve individuals in the information exchange, but which rely on personal information disclosed in other circumstances. For example, any given online activity is likely to involve disclosure of numerous types of personal data, sometimes over an extended or continuous period. The data collected through these activities is likely to be stored for an extended period and may be put to a variety of uses in the future.[28] Digital data that underpins this information can be categorised as three main types:

- **volunteered**—that is, data created and explicitly shared by the individual, such as data posted on social networking services (SNSs)
- **observed**—includes data harvested about an individual, such as their current location, or data harvested from third parties, such as an individual's purchasing history
- **inferred**—individuals volunteered and observed data that is processed to produce a new source of information and anonymised data that relates to groups of individuals, such as groups of individuals who 'like' the same activity.

[26] ACMA commissioned survey May 2015.

[27] In the Privacy Act, 'personal information' means information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. It includes such things as an individual's fingerprints, retina prints, body samples or genetic characteristics. It excludes information about an individual that is contained in a publicly available publication.

[28] World Economic Forum, *Personal Data: The Emergence of a New Asset Class*, 2011, p. 9.

Current data practices now support the collection of inferred information about personal behaviour and preferences. This does not directly or indirectly identify a person and inferred data is a category of digital data that has ambiguous status within the privacy regulatory framework, compared with volunteered and observed data practices that have a more established history under existing regulation.

Some types of personal data activity do not appear to be covered by existing protections, because of the type of data being collected, the characteristics of the entity collecting the data, or other circumstances associated with an activity's supply chain. Clarity around applicable regulation for digital data and the responsibilities of entities involved in information collection, storage and transfer will be important in establishing confidence in the regulatory settings for IoT and M2M communications.

Another consequence of the changed nature of communications in an IoT environment is that M2M communication requires no human interaction in a communications chain. Regulation has traditionally relied on an individual or an entity to be responsible for particular behaviours or outcomes. M2M communication challenges the effectiveness of existing regulatory constructs that rely on individuals to take action to mitigate particular harms. This may have the effect of elevating the importance of design standards, as a way to build in desirable network reliability and address information security concerns.

Interoperability of devices and the information exchanged between devices is identified as one of the important success (or value-unlocking) factors for IoT. McKinsey & Company, in their analysis of global IoT developments, suggested that interoperability of devices and IoT systems is needed to unlock approximately 40 per cent of the potential value of IoT applications.[29]

Regulatory settings have traditionally facilitated interoperability through registration of standards that are generally developed by industry groups. In Australia, this industry-led model has been successfully adopted in the past to address interoperability requirements of voice and data services. Drawing on this experience provides a platform for industry operators in the IoT environment to further develop interoperability requirements for information and devices.

Solving privacy, reliability and interoperability concerns may elevate the importance of standards-setting and design controls—not only for devices, but also for information exchanged between machines, as critical components in a successfully functioning highly-connected networked environment.

Digital data and cloud storage

The capacity of cloud computing for data storage is another pre-requisite for IoT applications, but with the utility of cloud storage predicated on the availability of high-capacity fixed and mobile networks to enable the near continuous collection and transmission of data from connected devices.

In Australia to date, there has been continued growth in the amount of digital data generated and downloaded by individuals, and an increasing take-up of cloud computing services. In the six months to May 2014, 14.2 million adult Australians

[29] McKinsey Global Institute, *The Internet of Things: Mapping the Value Beyond the Hype*, June 2015, p. 4.

(79 per cent) used a cloud service and an increasing range of cloud-based services is also being used.[30]

M2M communications and IoT applications will add to this volume with data generated between devices and machines. The capacity to transfer and store large amounts of data between different device types may be better facilitated by standards that establish common protocols for the transfer and portability of data, than by any direct regulatory approach. Telecommunications industry participants in Australia have experience in establishing porting arrangements for other services, so may have valuable experience to bring in establishing an optimal IoT environment.

Citizens and consumers making complex connections

ACMA research has documented the changing digital practices of Australians. Engagement with digital communications and content has intensified over the past 10 years, as people download increasing amounts of data, actively embrace cloud services for data storage, conduct more activities online, and connect as digital workers and digital consumers.

The ACMA is observing the continued evolution of media and communications transitioning to over-the-top (OTT) content and communications services. This is accompanied by strong differences emerging in consumer and citizen behaviour between different demographic segments, in particular reflecting the high take-up of new and emerging communications and content services by younger age groups.

Another development enabled by IP networks and devices is the capacity for individual consumers to initiate decentralized modes of network connection. The expanding take-up of OTT services is enabling consumers to use the communications 'building blocks' at network, service and device levels, to construct their own communication access pathways. Citizens and consumers can often choose a different option if one service is not working, effectively building additional redundancy and robustness through self-management of their communications network and service access. These decentralised modes of connection mean industry, government and regulators may need to address the existing public interest outcomes, such as end-to-end connectivity and universal service in new ways.[31]

The method of accessing the internet is also changing, with 70 per cent of Australians using a mobile phone to go online and 50 per cent using a tablet.[32] While the home is still the preferred place to connect to the internet, increasingly Australians are going online from alternative locations such as the workplace, wireless hotspots or a friend's place.

In managing multiple devices at home, there is a trend towards more complex home networks, as multiple devices connect to the internet by fixed line and Wi-Fi networks. While there are some challenges in managing the interaction of complex device connections, the building of such skills and familiarity with smart home IoT applications like energy management, may build the confidence of individuals in managing additional IoT applications more generally.

There is also evidence of an increasing fragmentation of activity, with Australians of different ages using the internet in markedly different ways. More than nine in 10

[30] Due to a change in methodology, this figure has been revised from 80 per cent as published in ACMA *Communications report series, Report 2—Cloud computing in Australia,* 2014.

[31] ACMA *Six emerging trends in media & communications*, November 2014.

[32] ACMA *Australians' digital lives*, March 2015.

(92 per cent) adult Australians used the internet in the six months to May 2014, including 100 per cent of the 18–44 age group, while younger adults (18–24 years) are the most active digital citizens and are much more likely to share files and content online.

Key enabling strategies

Given these key enabling characteristics of IoT as a global connection of things, people and data, it is likely that enabling or facilitative regulatory strategies will be more appropriate in circumstances where the intended outcomes are to:

- improve service standards
- understand obligations
- provide incentives for behavioural change by industry participants or citizens and where the regulatory framework remains unchanged or outdated.

Intrinsic to the adoption of enabling strategies is an acknowledgement that regulatory arrangements should be supportive of innovation and create deterrents to risky or harmful behaviours. Key strategies that are expected to be useful in this context include the following:

1. **Harmonisation**—the global connection of things, people and data underscores the importance of international frameworks to the development of any national regulatory arrangements. Harmonisation can be an effective strategy on a number of levels.

   Participation in international standards making bodies can develop a more certain operating environment to allow M2M and IoT applications to develop. For example, Australia participates in ITU-R World Radiocommunication Conferences that identify and plan for harmonised spectrum bands that may be used for M2M and IoT applications, and also monitors the International Telecommunications Union Telecommunications standards groups that establish communications protocols.

   Another aspect of harmonisation relies on the sharing knowledge and experience with and between other regulators, law enforcement and industry groups to build cooperative mechanisms and identify best-practice approaches that may include non-regulatory as well as regulatory responses.

   Together, these various harmonisation activities help build certainty in the operating environment for emerging applications such as IoT.

2. **Forbearance**—in an environment where the market is rapidly changing, where a problem may be temporary, or where the costs of intervention are uncertain relative to the intended benefits, a decision to not take regulatory action or forbear can be important to removing an impediment to action, as well as providing the opportunity for industry participants to develop a solution to an issue.

   Forbearance can be understood in two ways—first, as a regulatory policy position, and second, as a response to an individual breach of applicable law. Regulatory forbearance may be adopted as a short-term measure while other legislative solutions or regulatory approaches are being developed, or to allow industry time to come to terms with new obligations. There may also be other circumstances where such an approach makes sense for reasons of proportionality, including fairness and the costs and benefits of undertaking enforcement action. A key benefit of this approach is the clarity it can provide to a developing industry about the scope of application of regulation.

3. **Use of alternatives to direct regulation**—in the communications and media regulatory framework, the explicit recognition given to industry co- and self-

regulatory arrangements provides a key mechanism for addressing issues of concern to industry participants in an environment of change.

Strategies such as program-based responses may be developed by industry participants or industry participants working in conjunction with the regulator. Program-based responses have been particularly useful in the past in addressing aspects of citizens' internet-based activity—for example, the Australian Internet Security Initiative, which addresses network security risks arising from malware infected computers. This type of program-based response may provide a useful template as a way of addressing harms that require some form of industry or citizen behavioural change to mitigate a risk.

Similarly, market-based strategies using incentives may be helpful where the desired outcome is to promote or deter particular forms of industry or citizen behaviour. Market-based strategies may be developed by the regulator but equally, could be developed by industry participants using the current co- and self-regulatory constructs of the Australian regulatory framework.

4. **Communication and information provision**—communication strategies are particularly useful where improvements in knowledge, or industry and citizen behaviours are the intended outcome, and they provide a flexible response to addressing emerging issues.

   In the IoT environment of complex connections, one of the chief benefits of using communication strategies is that they clearly recognise the role of citizens and industry participants as problem-solvers in a globally connected online environment.

   Communication activities also provide a feedback mechanism from industry and the community about emerging issues of concern or risk, and have the benefit of allowing for a highly-targeted intervention to a particular segment of the population.

   The type of strategies that may be used include public information and education campaigns, which are useful when the problem to be addressed concerns a lack of knowledge. Information disclosure is another more targeted strategy directed to the provision of standardised information or guidelines, usually concerning a particular product or activity.

Problem-solving strategies

As M2M and IoT applications become more widely available and used, more evidence will become available of the benefits of IoT, as well as a clearer view of where the potential inhibitors to supply and use may be, or where areas of risk are emerging. The highly dynamic nature of IoT communications means that an effective response often requires finite resources to be directed to the issues posing most risk or those having the most significant impact on business and citizens—that is, systemic risks. There are a number of relevant strategies that assist in identifying the nature of the problem that may require attention. These include:

1. **Conducting research**—Identifying the scope and scale of an issue, while simple in theory, is expected to become more difficult with complex connections and information flows under IoT. Research (either by policy departments, the regulator or by industry participants) to establish the dimensions of an issue and its risk profile, will be an important first step in any problem solving approach. Determining whether an issue requires regulatory attention is informed by whether the issue:
   - is regarded as significant
   - is clearly established
   - may be solved by market-based solutions in time

- interferes with market incentives
- raises costs of intervention that outweigh the identified benefits.[33]

2. **Conducting inquiries**—this is another strategy available to a regulator to build evidence and inform stakeholders about the type of response to an issue that may be required.

3. **Collaborative partnerships**—in the complex connected environment of IoT, problem-solving strategies will also necessarily rely on a mix of participants. For this reason, collaborative partnerships between industry, government, citizen or consumer stakeholders will be increasingly important to the design of any regulatory or non-regulatory initiatives. This approach is designed to develop effective intervention by engaging multiple parties, undertaking collaborative agenda-setting, using moral persuasion, and designing an effective intervention that takes account of the self-interest of the industry or citizen participants.

4. **Better use of existing regulation**—internationally, regulators are reviewing regulatory frameworks in light of market and technology developments. In the United States, the Federal Trade Commission has focused on the demand-side consumer aspects of network security and user privacy policies relevant to the IoT environment. The recent net neutrality rules announced by the US Federal Communications Commission focus on the supply-side rules for an open internet that will support IoT. In the United Kingdom, Ofcom has signalled an interest in the enabling infrastructure policy initiatives in spectrum and addressing policy that support M2M and IoT communications. A common thread evident from these various initiatives is the focus on the better use of existing regulatory provisions that incorporate different aspects of the following response strategies. This includes an assessment of whether:
   - existing regulation can be extended to apply to the new market circumstances
   - existing regulatory tools can be repurposed to accommodate a change of emphasis or application to a different set of market activity or industry participants
   - regulation needs to be removed
   - there is a need for a complete redesign of regulatory frameworks and tools.

The hyper-connectivity envisaged by the IoT is expected to further test existing regulatory structures and the toolkit available to industry participants and to the regulator to facilitate and respond to the emerging issues associated with M2M and IoT adoption. While enabling and problem-solving strategies are expected to form an important part of the future toolkit for IoT, there will need to be a longer-term consideration of whether regulatory structures remain fit-for-purpose for an IoT environment.

[33] ACMA, *Connected citizens—A regulatory strategy for the networked society and information economy*, p. 15.

Part 3—Areas for regulatory attention

This part looks at the implications of IoT developments for the sectors regulated by the ACMA and assesses the key policy settings or enduring concepts relevant to facilitate productivity benefits from IoT, including whether they remain fit for purpose. It is intended to offer a framework for analysis when considering whether existing regulatory settings either support or potentially inhibit developments in M2M and IoT. This style of analysis may prove helpful when considering whether any regulatory intervention is necessary.

Implications of IoT developments for the sectors the ACMA regulates

The ACMA's experience is that each of the four sectors it regulates is facing different pressures, as IP-enabled communications and content evolve.

In **telecommunications**, the growing shift to mobile and data-driven communications, together with the changes in market structure that will flow from the nbn, is providing a network and device capability that will underpin M2M and IoT developments. This also means that many aspects of Australia's existing fixed-voice regulation are increasingly concerned with solving legacy problems. As telecommunications devices evolve, we could expect increased attention focussed on telephone numbers that support M2M and the telecommunications standards and protocols that will set the design features enabling IoT.

In the **broadcasting** sector, there are new regulatory challenges now that the digitalisation of broadcasting networks is complete. The digitalisation of content and the shift to online content delivery models, with increasing potential substitution between print, broadcast and online content, raises a fundamental challenge in considering whether content safeguards remain relevant, and whether and how content production support models can be maintained in a more contestable digital content environment.

In **radiocommunications**, the recommendations from the Spectrum Review provide a path for modernising Australia's spectrum management framework, including the simplification of the licensing framework. Spectrum's enabling role as a key input to M2M and IoT applications is expected to generate increased attention in international planning forums like the ITU-R World Radiocommunication Conferences. At the domestic level, pressure from those seeking access to already utilised spectrum will likely see a continued need for regulator involvement in band replanning and allocation.

In the **online environment**, M2M and IoT is expected to accelerate many of the current challenges experienced by citizens and regulators that arise from global information flows and rapidly changing user behaviours. The ACMA's experience is that direct regulation at a national level has limited capacity to respond to multi-national information flows. Maintaining international engagement and building multinational partnerships are key strategies that assist the ACMA and industry to take collaborative action in relation to online issues. Educating and informing citizens and business about productive engagement within the IoT environment is also expected to remain an important response strategy.

There are many uncertainties about how the impact of the scale of mass connectivity and speed of change will affect the Australian communications and media sectors and the regulatory environment.

One of the key challenges arising from the mass global connectivity envisaged under IoT and IoE is that the network, device, information and people ecosystem is no longer closed—in practical terms, expanding the field of unregulated activity. While this may pose no immediate reason for regulatory attention, it is important to be aware of the impacts on current regulation, and whether this has the effect of facilitating or hindering innovation.

In general terms, existing regulatory structures have relied on relatively 'closed' systems identifying known industry participants (mainly using licensing systems) to deliver specific policy outcomes. The globally-connected nature of information, devices and people under M2M and IoT also erodes the effectiveness of any nationally-based regulatory schemes, pointing to the need for increased international cooperation to achieve specific outcomes.

At this stage of Australia's transition to IoT, it is useful to examine whether existing regulatory settings are likely to assist or hinder the wider adoption of M2M and IoT.

A framework for analysis

To further inform this analysis, the ACMA has looked at the conceptual underpinnings for regulatory responses in communications and media markets. The ACMA's earlier analysis of convergence impacts on communications and media regulation set out in *Enduring concepts* sought to identify those concepts of ongoing importance in media and communications in Australia. It considered the fundamental concepts that describe the policy objectives for present regulatory intervention in communications and media, and assessed whether they inform the basis for any future intervention.

This style of analysis can also be applied to assessing how existing regulatory settings support or inhibit developments in M2M and IoT:

1. What is the public interest to be served or the problem to be solved by a particular objective or intervention?
2. What is the current method employed to serve the public interest or solve the problem?
3. Does the public policy good still warrant support or the problem still need solving?

To identify the sorts of practical outcomes that may need to be delivered to support M2M and IoT in the future, a further query arises:

4. Whether the capacity to achieve the policy objective can continue in an IoT environment, including whether:
   - existing interventions could be extended to IoT
   - existing interventions should be lessened on entities utilising application of IoT or other related market participants (data miners, analytics marketing/advertising companies)
   - existing interventions should be applied in different ways to remain an effective problem-solving intervention.

To illustrate some of the types of regulatory design issues that arise, this analysis has focused on the 'enduring concepts' regarded as of most relevance to the mass connectivity of M2M and IoT, namely:

- market standards (competition, quality, redress and efficiency)

- social and economic participation (access, confidence and digital citizenship)
- safeguards (protection of the public, digital information management and national interest objectives).

The ACMA's previous analysis also identified five regulatory concepts related to content and cultural values (diversity of voices, Australian identity, community values, localism and ethical standards and the safeguards related to protection of children from age inappropriate content). These regulatory concepts reflect different aspects of Australian cultural values that are less relevant in the context of IoT communications, and so they are not considered further here for this analysis.

The analysis identified that the main public policy objectives that underpin market standards, social and economic participation and safeguards remain relevant in an IoT environment characterised by complex connections, highly distributed and adaptive networks, and rich data.

However, the method for achieving these objectives is likely to require revision to rebalance the focus of regulatory attention in a way that will provide more effective support for M2M and IoT developments. For example, efficient allocation of spectrum and telephone numbers to promote access to innovative services, enhancing quality standards through a focus on network reliability and device standards specification, supporting effective participation through business and consumer skills development and safeguarding the security of digital information to encourage confidence in the IoT environment.

A rebalancing of focus within the regulatory framework to support mass connectivity is not to suggest that every intervention is necessary or necessarily a regulatory one, but detailed analysis of where the appropriate future balance lies between direct regulation, industry co- and self-regulation, and non-regulatory responses is required.

Table 1: Enduring communications policy objectives relevant to IoT

IoT enablers	Relevant concepts	Can the objective continue to be met in the IoT environment?
1. Infrastructure	Competition	The traditional focus has been on competitive access to infrastructure through which communications services are supplied. Will this achieve the following outcomes in an IoT environment? - services competition - any-to-any connectivity for services that involve communications with end users. The concept of any-to-any connectivity is emerging as a key concept that will underpin the complex connections of IoT - encourage efficient use of, and investment in infrastructure including through access to public resources. Competition-related aspects of digital information that enable IoT is an emerging area of attention concerning: - the degree of control that network operators may exercise over the carriage of data on their network (net neutrality issues) - the extent to which device interoperability and the availability of data portability features will facilitate competition and choice.

IoT enablers	Relevant concepts	Can the objective continue to be met in the IoT environment?
	Efficiency	In the IoT infrastructure context, this concept remains relevant to > ensure the efficient allocation and use of public resources > ensure the efficient operation of, and investment in, communications networks. A continued role for licensing as a method is likely to remain where this is related to the management and efficient allocation and use of finite public resources such as spectrum. IoT applications that do not rely on these resources will sit outside the regulated sphere of activity, where licensing is used as a construct to manage the efficient operation of markets and market participants.
	National interest	Defence, security and law enforcement agencies are likely to continue to have requirements in the IoT environment to protect the security of Australia. Complex IoT connections potentially greatly amplify the impacts of any network or national security breaches. A heightened interest in device and network security and reliability may require new technological solutions and/or standards specification to address the interception and access requirements of law enforcement and national security agencies.
2. Devices	Quality	While quality objectives have a number of different dimensions in communications and media regulation, the elements most relevant to IoT concern quality standards relevant to technical and product performance in service delivery. These quality standards are primarily achieved by network performance and device standards and licence obligations in current regulation. The methods for delivering these quality objectives are currently tied to specific licence and service types, but provide a basis for further enabling IoT applications, primarily through the specification and harmonisation of device standards. There are benefits to device manufacturers where harmonised standards can provide economies of scale that realise lower cost devices.
	National interest	As noted above, device standards are likely to play an important role in meeting the national security and law enforcement objectives in the connected IoT environment.

IoT enablers	Relevant concepts	Can the objective continue to be met in the IoT environment?
3. Data and information	Quality	Another dimension of quality objectives is information standards that, in the IoT context, are likely to be concerned with the provision of consumer product information. In the IoT environment, the requirement for seamless transmission of large quantities of information between devices may require additional attention to the underpinning standards needed to support information transfer. Certainty also needs to be given to providers of information about how such information will be collected, transmitted and stored, including the treatment of personal information and privacy protections.
	Digital information management	The integrity of personal information, and the interoperability of devices and portability of data and information, will be key underpinnings for the IoT environment. Three elements of this concept may require further examination in the IoT context to provide certainty for suppliers of IoT services about their obligations, as well as certainty for users in supplying information that is exchanged in M2M and IoT communications. These elements include: > how much control should be available to network operators over the carriage of data over their networks (for example, packet inspection) > how service providers and other rights-holders store, retrieve and use personal data provided to them by users > device interoperability and portability of data between devices and networks.
	Protection of the public	Three elements of this concept that are identified as being of most relevance to IoT include: > access to emergency services to protect life, health and safety. In a highly networked environment, IoT applications may become another platform for general communications including accessing emergency services > protection from harmful communications (including unsolicited electronic messages). The application of anti-spam regulation will depend on whether the IoT communications path includes an electronic message component. The volume and complexity of M2M and IoT connections is expected to challenge anti-spam rules that rely on the ability to identify the sender of a message > prohibition of radio emissions likely to endanger safety. As wearables (including devices and clothing) embed IP-communications receivers and transmitters in their design, emission standards to protect individuals will become an increasingly important feature of wearables design.

IoT enablers	Relevant concepts	Can the objective continue to be met in the IoT environment?
4. People	Access	The concept of citizen access to basic communications services —and the related concept of any-to-any-connectivity—has supported social and economic participation in Australia. While various subsidy, affordability and price control regulations have been the key mechanisms applied to particular technology and service types that have been used to support this objective to date, the magnitude of connections made under IoT will potentially elevate the importance of access objectives to ensure that Australians are able to productively engage with IoT opportunities. Access in the IoT environment is predicated on the technical proficiency of users in being able to use devices, identify sources of services and manage digital information. These factors suggest a stronger emphasis in the future on the importance of citizen skill initiatives to enable access to IoT.
	Redress	The concept that there are appropriate avenues for dispute resolution, to allow users meaningful rights of complaint and redress, is expected to remain important in the IoT services environment. There are established redress mechanisms within current communications and media regulation. However, the broadening of IoT applications across the economy, underpinned by complex connections and supply chains, brings into question whether there will be effective redress mechanisms for the suite of IoT applications available.
	Confidence	Confidence in predictable regulatory settings is an important feature to enable the development and take-up of new communications services. IoT developments will magnify two processes that are challenging confidence in the capacity of existing regulatory settings to provide clearly defined obligations and rights, namely the globalisation of communications networks and information exchange, and decentralised modes of communications between end users. Each challenge regulatory models predicated on known entities and control points. The IoT environment is placing an increased emphasis on the role of international harmonisation for standards setting that will enable Australians to access low-cost devices and standardised applications. In addition, it offers an opportunity to focus on the development of skills and confidence of end users, so that they can operate productively in shaping their connections and information exchange in the IoT environment.

IoT enablers	Relevant concepts	Can the objective continue to be met in the IoT environment?
	Digital citizenship	The notion that Australians should have the technical proficiency and digital literacy for effective engagement in economic, social and civic life is closely linked to the regulatory concept of access. Skills that are expected to become more critical in the IoT environment, as business and individuals manage multiple devices and complex connections in daily life, will include some technical proficiency, as well as managing security settings, identity and authentication requirements, and the digital footprint created by IoT communications.

This analysis has focused on the capacity of existing communications and media regulatory settings to accommodate (and promote) M2M and IoT developments. However, the spread of IoT applications across health, transport, energy, smart cities and the connected home environment has accentuated the role of IP-enabled communications as a general purpose technology in the economy, which will benefit from specific attention within a coherent communications regulatory framework.

Based on an initial analysis, the ACMA anticipates that the balance of regulatory interventions in the future is likely to skew more towards the enabling strategies of facilitation and communication tools that, in the short term, aim to encourage innovation and the adoption of M2M and IoT applications.

Over time, as M2M and IoT applications become more mainstream within in the Australian economy and society, any particular risks or problems occurring in the supply and use of IoT applications will become more apparent. This suggests that a focus on problem-solving strategies may become more necessary over time to supplement the initial focus on enabling activities.

Conclusion

Australia has many elements of IoT enablers in place in its communications and media sectors. Each of the sectors the ACMA administers faces different sets of pressures in the transition towards an IoT environment.

While the rate of change and the complexity of connections that may occur with the IoT is currently unknown, the key areas of resource allocation for communications infrastructure planning, network integrity, device standards and information reliability—along with the digital capabilities of Australian business and consumers—remain important areas for an early focus on regulatory attention on enabling and facilitating the development of IoT in Australia.

In particular, the ACMA is interested in views from stakeholders on the following:

1. The ACMA would welcome any proposals from industry around the need for the designation of a discrete numbering range for M2M or IoT.
2. The ACMA would welcome views from industry about future spectrum requirements to support M2M and IoT applications.
3. The ACMA would welcome input from industry as to how cooperative models of information sharing and action by industry, citizens and regulators might be adapted to address newer forms of digital information harms.
4. Are there any additional issues that should be included as priorities for regulatory attention that have not yet been identified in this paper?
5. Has the ACMA correctly identified the near-, medium- and longer-term priorities for regulatory attention?

The ACMA appreciates responses and feedback on the questions it has raised throughout this paper, which will assist it to refine its priorities and identify where attention is needed to further facilitate the development of M2M and IoT applications in Australia.

researchacma

Canberra
Red Building
Benjamin Offices
Chan Street
Belconnen ACT

PO Box 78
Belconnen ACT 2616

T +61 2 6219 5555
F +61 2 6219 5353

Melbourne
Level 32
Melbourne Central Tower
360 Elizabeth Street
Melbourne VIC

PO Box 13112
Law Courts
Melbourne VIC 8010

T +61 3 9963 6800
F +61 3 9963 6899

Sydney
Level 5
The Bay Centre
65 Pirrama Road
Pyrmont NSW

PO Box Q500
Queen Victoria Building
NSW 1230

T +61 2 9334 7700
1800 226 667
F +61 2 9334 7799