Australian Government

acma

Australian Communications and Media Authority

researchacma
Evidence that informs

Internet of Things in media and communications

Occasional paper

JULY 2020

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

Australia's communications and media environment continues to undergo significant change, driven by new technologies and evolving consumer expectations. Over the past decade, the Internet of Things (IoT) has emerged as a key driver of change, transforming business models and consumer experience.

While not limited to any specific technology platform, industry, object or device, IoT relates to multiple wireless and wired interconnections of personal, consumer and industrial devices supporting a diverse range of applications. The data generated by IoT devices is enabling new insights, particularly when combined with advanced analytical capability.

Consumer IoT applications such as wearable devices are allowing consumers to monitor daily exercise and sleeping patterns. Smart home applications are supporting consumers to enhance household efficiency and effectiveness by improving accessibility, security and energy efficiency.

Industrial IoT applications are transforming Australian industries. Industrial IoT applications are optimising business processes, increasing performance and reducing costs. Applications such as connected factories are improving productivity and process flows. Smart sensors, which continuously monitor machines, buildings or equipment, are improving productivity and reducing business costs.

The IoT market in Australia is growing rapidly, with industry research estimating the value of IoT at close to $19 billion in 2018 and growing to $30 billion by 2023.[1] The continued rollout of 5G networks is expected to spur further IoT growth.[2]

This paper explores the impacts of IoT across the media and communications environment. It examines the key components of IoT, consumer and industry applications, market and usage trends, key challenges and the implications for our regulatory environment. It identifies regulatory touchpoints and activities planned or underway to support the ongoing development and deployment of IoT within Australia.

This work builds on existing research into IoT and discusses a range of issues to help ensure the ACMA's regulatory settings and strategic direction are appropriate for current and future IoT developments.

[1] PwC, *Australia's IoT opportunity: Driving future growth, An ACS report*, September 2018, p. 10.

[2] Department of Communications and the Arts, *5G - Enabling the future economy, October 2017*, p. 8.

About the research

This paper outlines the ACMA's next steps for IoT and potential regulatory directions to meet the short-, medium- and long-term challenges posed by IoT within the context of a dynamic and evolving media and communications environment. In producing this paper, we conducted research that considered:

- current and anticipated market developments in the deployment of IoT within an Australian context
- international and domestic regulatory developments relating to IoT.

We consulted with select Australian Government agencies and key IoT stakeholders. Feedback from this consultation informed the development of the paper.

research**acma**

Our research program—researchacma—underpins our work and decisions as an evidence-informed regulator. It contributes to our strategic policy development, regulatory reviews and investigations, and provides a regulatory framework that anticipates change in dynamic communications and media markets.

This paper contributes to the ACMA's market developments and regulatory best practice and development research themes, reflecting the importance of IoT as an enabling technology. This paper provides some insights into how future regulatory developments could provide a supportive environment for IoT applications. More details can be found in the ACMA research program.

Introduction

The Internet of Things (IoT) is a significant driver of change within the markets regulated by the ACMA and across the broader economy. The growing reach of IoT is driving behavioural change in how consumers interact with machines and networks. It is also supporting industries to find new ways to improve productivity and efficiency.

Identifying the opportunities and challenges posed by IoT, and ensuring our regulatory framework is fit for purpose, is important to ensure Australia realises the full economic and social benefits of IoT. Proactive engagement with consumers and industry can facilitate greater trust and acceptance of emerging technologies, such as IoT.

IoT intersects with several elements of the ACMA's regulatory framework including network infrastructure, consumer safeguards, equipment standards and spectrum management.

The ACMA is responsible for managing Australia's radiofrequency spectrum and ensuring it is managed in a way that maximises the overall public benefit derived from its use. As spectrum use and demand drivers continue to evolve, we are regularly monitoring the environment to ensure we have an accurate understanding of changes in technology, consumer preferences and market demands, including IoT.

This paper discusses a range of issues to help ensure our regulatory settings and strategic direction for IoT are appropriate, given current and anticipated future developments.

Scope of this paper

This paper explores the impacts of IoT across the media and communications environment. It examines the key components of IoT, consumer and industry applications, market and usage trends, key challenges and the implications for our regulatory environment. It identifies activities planned or underway to support the ongoing development and deployment of IoT within Australia and highlights potential areas for action over the medium- to long-term.

In this paper, we have focused on the areas of our regulatory remit that intersect closely with IoT:

- network infrastructure
- spectrum management
- equipment standards
- consumer safeguards.

The paper is focused on pressures relating to the regulatory environment the ACMA administers. It does not address challenges that sit outside our remit.

What is the Internet of Things?

From a conceptual standpoint, IoT is that ability to create digital awareness of the physical world we live in. It's a digital pulse made up of data that we can aggregate to improve the world around us.
John Rossman[3]

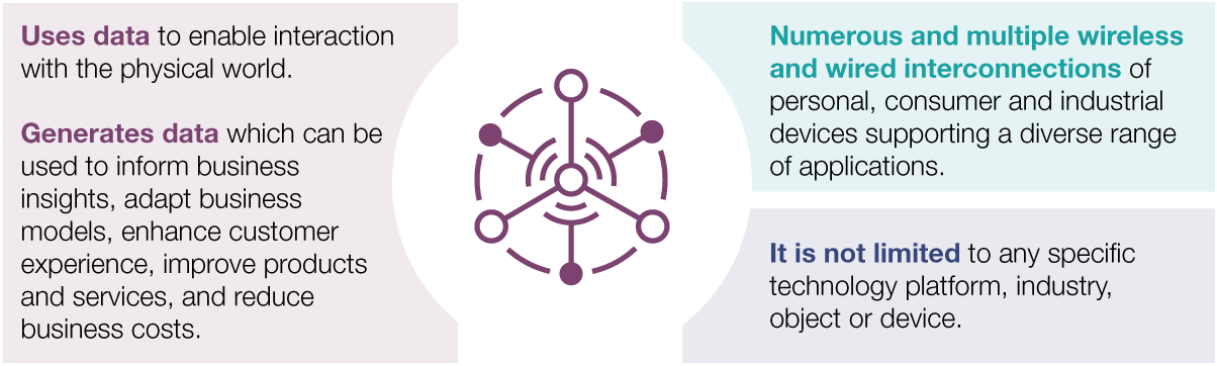
IoT is a network of connected things and people. It collects and shares data about the way an IoT device is used and the environment around it. It is an intelligent global network connecting a multitude of devices from wearables, medical sensors, vehicles, appliances, infrastructure and other objects, which are integrated with technology such as sensors, software, and actuators, enabling these devices to operate more efficiently and effectively.

The ACMA's draft *Five-year spectrum outlook 2020–24* describes IoT as:

> … the interconnection of many devices and objects utilising internet protocols, with or without the active involvement of individuals. This may include laptops, routers, tablets and smartphones, which are integral to operating, reading and analysing the state of IoT devices.[4]

IoT is not limited to any specific technology, platform, device or use case. Figure 1 shows some of the key features of IoT.

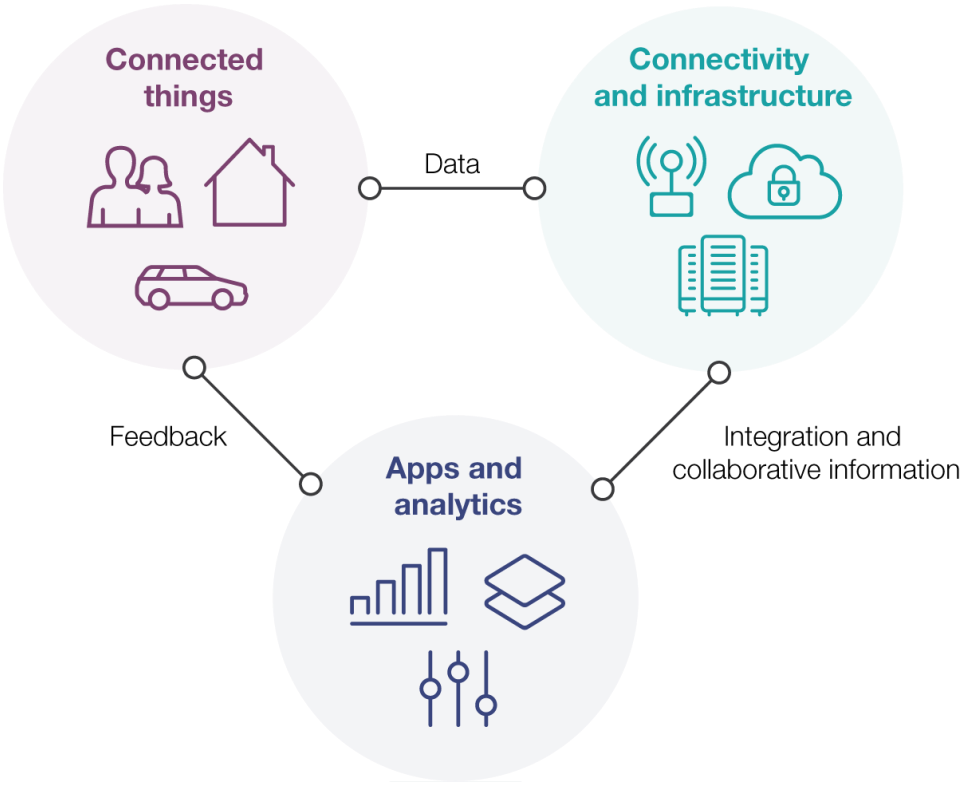
Figure 1: Common features of IoT



Ericsson forecasts that by 2022, there will be 18 billion IoT connected devices worldwide.[5] Building on this, we see IoT as involving *unprecedented numbers of wireless and wired interconnections of personal, consumer and industrial devices supporting a range of applications.*[6] This is illustrated in Figure 2.

[3] John Rossman, *The Amazon way on IoT; 10 principles for every leader from the world's leading Internet of Things Strategies*, Clyde Hill Publishing, 2016, p. 1.
[4] ACMA, draft *Five-year spectrum outlook 2020–24*, April 2020, p. 26.
[5] Ericsson, *Internet of Things Forecast*, 2018.
[6] ACMA, draft *Five-year spectrum outlook 2020–24*, April 2020 p. 26.

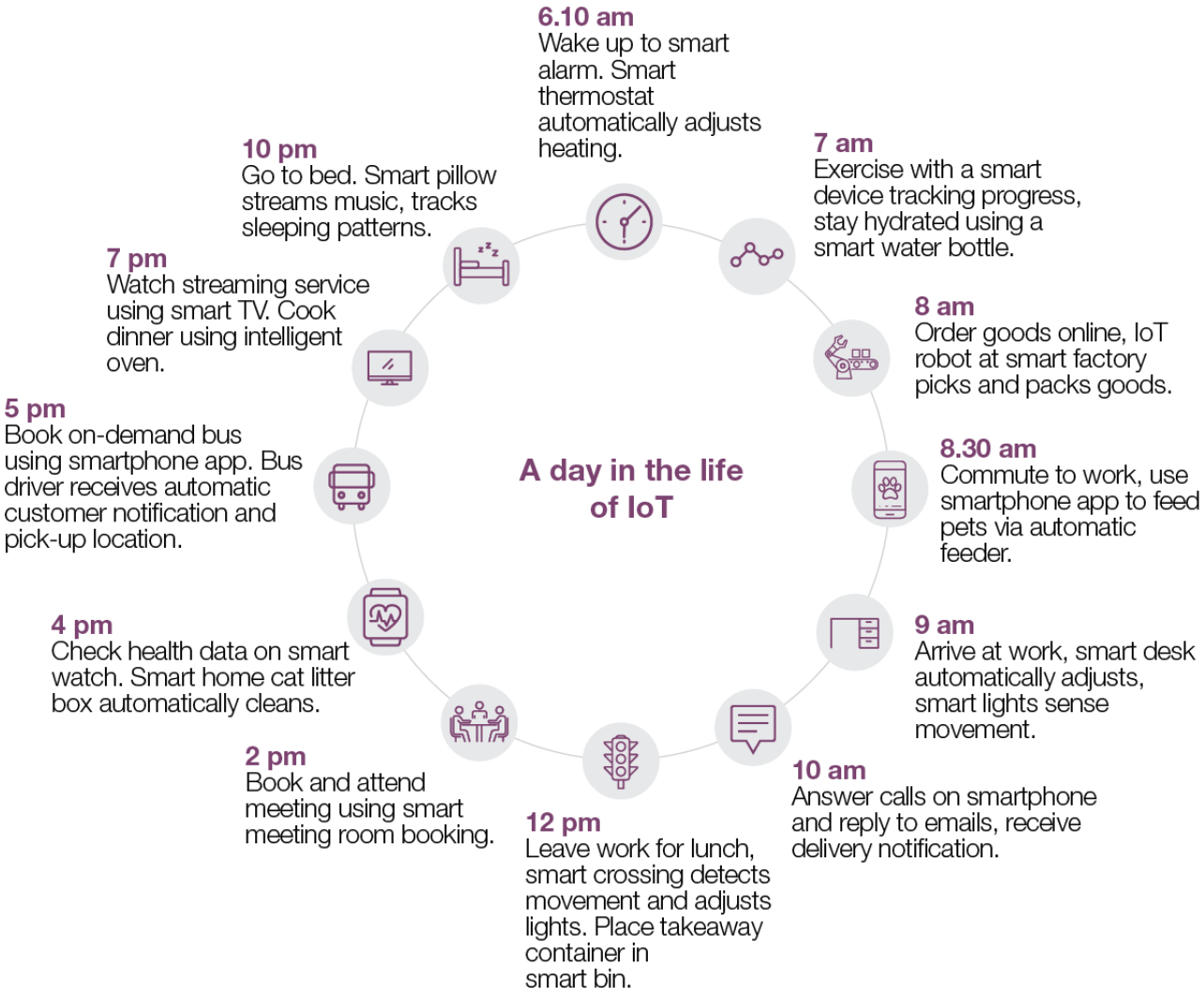
Figure 2: The IoT



Adapted from Mimos Berhad, National Internet of Things Strategic Roadmap: A Summary, 2015, p. 4.

IoT applications vary in complexity and use cases, as shown in Figure 3. Consumer IoT devices range from the relatively simple, such as a smart key-finder, to premium smart home automation applications. Industrial IoT applications are generally more complex and include the use of IoT within industrial sectors and applications such as predictive maintenance, which enable companies to identify potential failures and increase production.

Figure 3: A day in the life of IoT



Source: ACMA, 2020.

It is estimated there are currently more connected IoT devices than people.[7] Low-cost sensors and high-bandwidth wireless networks are enabling more devices to be connected, monitored and tracked, to share data on their status and to communicate with other devices. This data generated by connected devices can be collected and analysed to improve production efficiency. IoT is also an important enabler of intelligent and connected smart homes, offices, cities and regions. Table 1 highlights common uses for consumer and industrial IoT.

[7] Gartner, *Gartner Identifies Top 10 Strategic IoT Technologies and Trends, 7 November 2018*, forecasted there would be 14.2 billion connected IoT devices.

Table 1: Consumer IoT and industrial IoT

Consumer IoT	Industrial IoT
> Wearables	> Transportation
> Smart TVs	> Smart cities
> Smart bike locks	> Asset tracking
> Home monitoring	> Connected manufacturing
> Home automation	> Smart utilities
> Smart appliances	> Smart farming

Australia's IoT environment

IoT network availability

IoT devices use a range of different networks. In some cases, IoT device connectivity is served through domestic technologies for broader consumer networks, whereas others use bespoke technologies and dedicated network infrastructure.

IoT devices vary regarding technical requirements, in terms of whether the device is short- or long-range and whether it uses low, medium or high data rates. IoT connectivity requirements are application specific and have specific latency requirements as well.

Multiple IoT technologies are being deployed across Australia, including:

- **NB-IoT**
  NB-IoT is a commonly used IoT technology in Australia. NB-IoT is well-suited to communications in fixed environments. It is unable to carry voice communications. Within Australia, Telstra, TPG Telecom Limited (formerly Vodafone Hutchison Australia (VHA)) and Optus have deployed NB-IoT networks. VHA has estimated their NB-IoT footprint covers 89 per cent of the Australian population and supports applications such as aged care management and smart building services.[8]
- **LTE Cat-M1**
  LTE Cat-M1 uses existing 4G networks. As of September 2019, more than 3.2 million IoT devices were connected to the Telstra LTE Cat-M1 network.[9]
- **Sigfox**
  In Australia, Sigfox operator Thinxtra has continued to expand its networks, covering 87 per cent of the Australian/New Zealand population as of February 2019, supporting use cases including smart farming, smart logistics tracking and urban planning.[10]
- **LoRaWAN**
  LoRaWAN networks are being rolled out by a range of organisations, including municipal councils, utility providers and infrastructure companies. For example, the City of Gold Coast has deployed a LoRaWAN network that will enable the effective deployment of large scale IoT projects, including smart water meters and waste management.[11]
- **Satellite systems**
  Satellite systems enabling IoT services are also being pursued. Given the capabilities of satellite systems, several companies are delivering or pursuing new

[8] Hutchison Telecoms, *Annual Report 2018–19*, 30 July 2019, p. 6.

[9] Gerhard Loots, *Over 3 million new IoT 'things' on our network*, Telstra Exchange, 5 September 2019.

[10] Thinxtra, *IoT coverage where you need it, plug and play*, 7 February 2019.

[11] Georgia Clark, *Gold Coast unveils nation's largest digital network*, Government News, 20 May 2019.

space-based IoT services.[12] Some of these services are being deployed through established satellite bands. However, in some cases, enabling satellite IoT may require specific changes to the regulatory framework.

Value of IoT in the Australian market

IoT is having a significant impact within the Australian market for consumers and industry alike.

Today, IoT devices are found in over five million Australian households.[13] From smart door locks, smart thermostats, connected kitchens, smart security devices to smart Bluetooth trackers, IoT devices and capabilities continue to impact our daily lives. IoT in the workplace is improving efficiency and productivity within workspaces. Office buildings are becoming smart buildings with smart lights, motion sensors and smart desks.

The value of the IoT industry in Australia is significant. PricewaterhouseCoopers Consulting (PwC) estimated the total value of the IoT industry in Australia was worth close to $19 billion in 2018 and forecasts the value of the IoT industry in Australia to grow to $30 billion by 2023.[14]

IoT is also a growing revenue source within the telecommunications sector. Telstra reported its IoT business grew by 19.4 per cent in revenue in 2019, with an average of 2,000 IoT devices connecting to their IoT network every day.[15]

IoT is transforming a wide range of industries, including agriculture, logistics, manufacturing, utilities and healthcare. PwC examined potential annual benefits from IoT across five sectors in Australia, with estimations ranging from $22 billion to $96 billion per sector (Figure 4).

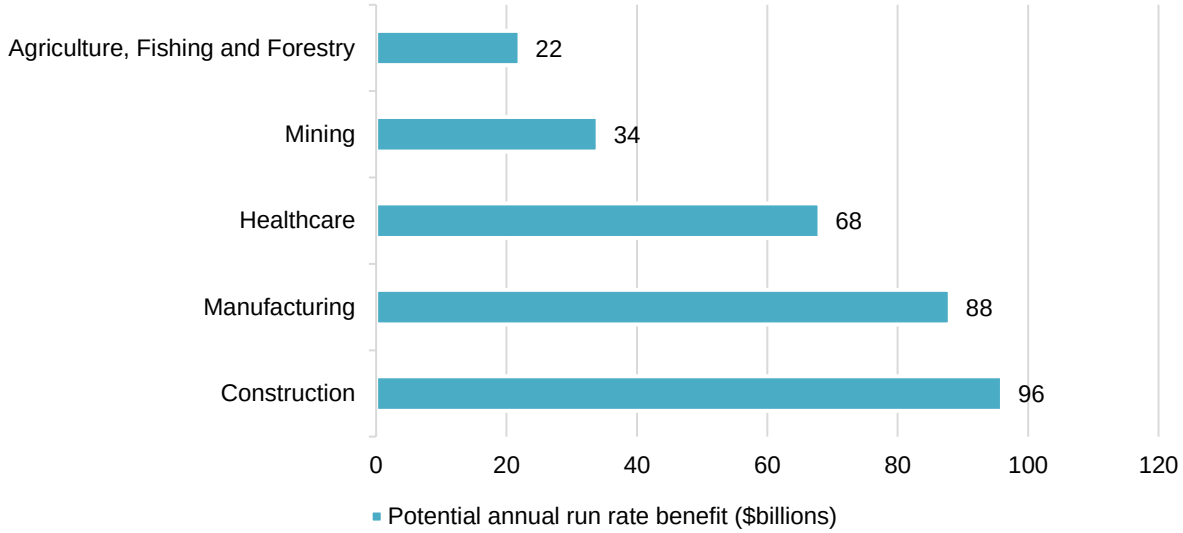
[12] An example is the Australian based start-up Fleet Space Technologies, which are implementing satellite-based systems for industrial IoT applications.

[13] Telsyte, *Australian IoT @home market cracks $1billion, paving the way for IoT commerce devices*, 14 May 2019.

[14] PwC, *Australia's IoT opportunity: Driving future growth, An ACS report*, September 2018, p. 10.

[15] Telstra, *A pivotal year: our 2019 results show strong progress on T 22*, 15 August 2019.

Figure 4: Potential annual benefits arising from IoT (2018)[16]



According to the International Data Corporation (IDC), almost half of Australian enterprises (46.5 per cent) have deployed at least one IoT solution and are planning on expanding their systems.[17] Globally, IDC forecasted significant levels of international investment in industrial IoT in 2019 and predicted the greatest levels of investment would include manufacturing operations ($100 billion), production asset management ($44.2 billion), smart home applications ($44.1 billion), and freight monitoring ($41.7 billion).

[16] Data derived from PwC, *Australia's IoT opportunity: Driving future growth, An ACS report*, September 2018, p. 9. This data projects annual benefits across a range of sectors over an eight to 18-year period.
[17] International Data Corporation, *Almost Half of Enterprises Launch IoT Solutions*, 20 January 2019.

ACMA's perspective on IoT in Australia

To date, the ACMA's focus has been directed towards ensuring our existing regulatory framework has the right conditions and settings in place to support IoT developments, along with identifying potential inhibitors to these developments.[18] This includes how IoT is interacting with the current consumer safeguards, such as interoperability of network devices, access to emergency services, privacy, and health and safety requirements.

International progress in IoT, such as the development of standards, is also being monitored. Globally, governments are facing increasing pressure to regulate, as public trust in technology requires reinforcement.[19] For the full benefits of digital technologies to be realised, regulatory settings need to balance necessary protections on issues such as privacy or security, with opportunities to enable innovation and market growth.

We are engaging with other regulators, standards bodies and industry groups to ensure our regulatory environment remains fit for purpose in a dynamic, increasingly digital environment.

In Australia, IoT intersects across various regulatory frameworks administered by different regulatory bodies. Within our remit, IoT has several touchpoints, which are described below.

Network infrastructure

The ACMA monitors and reports on efficiency of the supply of telecommunications services; the adequacy, reliability and quality of these services; and carrier and carriage service providers' obligations under codes and standards. Our remit includes setting technical standards for customer equipment and customer cabling and registering network industry codes relating to technical regulation of networks.

Reliable, accessible and effective telecommunications infrastructure is a key enabler of IoT. Typically, IoT devices connect via wireless networks. An IoT device could connect to the internet via a variety of methods including cellular, satellite, wi-fi, Bluetooth, low-power wide-area networks (LPWAN), Sigfox or connecting directly via ethernet. Table 2 describes some of the main IoT networks, network characteristics and IoT applications.

[18] ACMA, *The Internet of Things and the ACMA's area of focus, Emerging issues in media and communications- Occasional paper*, November 2015, p. 8.

[19] Edelman, Edelman Trust Barometer 2020, February 2020, p. 20.

Table 2: IoT wireless network options [20]

Network type	Low-Power Wide-Area Network (LPWAN)	Mobile network	Local/Personal Area Network (LAN/PAN)	Satellite
Range	High	High	Low	High
Bandwidth	Low	High	High	Low
Power use	Low	High	Low	Low
IoT applications	IoT applications include asset tracking, smart cities, agricultural and environmental monitoring and sensors	IoT applications include smart factories, fleet management, augmented reality	IoT applications include consumer applications, building automation, in house energy management	IoT applications include smart farms, mining, animal tracking, vessel tracking
Examples	> Sigfox > LoRaWan	> 3G, 4G and 5G for example NB IoT, Cat-M1	> ZigBee > Wi-fi > Bluetooth	> Myriota > Iridium > Starlink

Private networks are expected to grow with the increased availability of long-term evolution (LTE) advanced pro (4.5G) and 5G technologies. Private networks can provide companies with more control over the network, which may ensure greater regulatory compliance and security. As noted by Omdia, the growth in private networks is closely linked to the growth in industrial IoT, as private networks have been identified as a solution for sectors and environments with complex communication requirements.[21] Private networks have been used to support various industrial IoT applications, such as manufacturing, farming, and utilities.

As identified in the ACMA's draft *Five-year spectrum outlook 2020–24*, several network deployment models are currently in use by industry operators:

1. Using their own equipment and class-licensed spectrum to operate.
2. Using their own equipment and spectrum to run their own network (for example, public safety).
3. Having a private network built and designed by a third party (for example, a telecommunications company or network design business) with equipment sourced from vendors (for example, base stations and core network), which is separate to other mobile networks (for example, mining companies).[22]

[20] Adapted from the NSW Department of Customer Service, *Internet of Things Policy Guidance*, 15 October 2019, p. 144.

[21] Omdia, *Private LTE sets the scene for Industrial IoT and 5G test beds*, 12 April 2019.

[22] ACMA, draft *Five-year spectrum outlook 2020–24*, p. 26.

With the increased prevalence and uptake of IoT devices, we are monitoring whether the growth in data traffic impacts on network infrastructure. According to Cisco VNI forecast data, online traffic in Australia will grow three-fold from 2017 to 2022, a compound annual growth rate of 27 per cent, with M2M modules accounting for 5.7 per cent of IP traffic by 2022.[23] Cisco VNI data also indicates that in Australia, M2M modules will account for 62 per cent (161.6 million) of all networked devices by 2022, compared to 44 per cent (62.4 million) in 2017, a compound annual growth rate of 21 per cent.[24]

Spectrum management

The ACMA is Australia's spectrum manager and is responsible for ensuring radiofrequency spectrum is managed in a way that maximises the overall public benefit derived from using the spectrum.

Spectrum-related issues are a key part of the ACMA's interest in IoT, because IoT technologies are largely spectrum dependent. The diverse options for implementing IoT cover a wide range of technologies, spectrum requirements and models for accessing spectrum. Factors like the degree of complexity or criticality of an IoT application, or the physical environment it operates in, may influence decisions about how spectrum is accessed. This, in turn, may affect the way demand for spectrum evolves over time.

The ACMA's *Five-year spectrum outlook 2019–23* (FYSO 2019–23) identifies that advances in new technologies (including IoT) are a key driver of changes in spectrum use.[25] FYSO 2019–23 also notes that the ACMA is facilitating early access to the 928–935 MHz band for low-power wide-area (LPWA) IoT applications. The six-month progress report for FYSO 2019–23 indicates this work is ongoing.

Current deployments of IoT have mainly focussed on spectrum use where that spectrum is available at a low cost (or free). In Australia, this has primarily included access to bands that are governed by the Radiocommunications (Low Interference Potential Devices) Class Licence 2015 (LIPD class licence). The LIPD class licence is reviewed regularly and has successfully adapted to changing global market conditions by including additional frequency bands as required.

The next update of the LIPD class licence will take place in late (Q4) 2020. This update will include a range of proposed provisions for IoT networks, including implementation of the abovementioned LPWA arrangements in the 900 MHz band. The ACMA is also in the process of consulting on potential arrangements for IoT arrangements in the VHF band. Outcomes of this consultation process will further inform proposals for the forthcoming LIPD class licence update.

Broadband networks including 3G and 4G support IoT deployments. As outlined in the FYSO 2019–23, 4G and 5G standards are making—or have made—specific provisions for dedicated IoT service delivery.[26] IoT devices in use within Australia are currently utilising class-licensed bands, and multiple satellite systems are also in use or in development to enable IoT in a range of dedicated satellite bands.

It is expected that the rollout of 5G communication networks will support further IoT growth, especially for applications needing very high data rates and very low latency.

[23] Cisco, *Visual Networking Index: Australia 2022 forecast highlights*, accessed 18 November 2019.

[24] ibid.

[25] ACMA, *Five-year spectrum outlook 2019–23*, September 2019, p. 17.

[26] ACMA, draft *Five-year spectrum outlook 2020–24*, p. 26.

The ability of 5G networks to support a massive increase in device connections is expected to support future IoT deployment.[27]

The ACMA has facilitated the initial 5G rollout in Australia through the auction process for the 3.6 GHz band, which was completed in the second quarter of 2018. The ACMA is continuing to work towards the timely release of spectrum to support the 5G roll-out. In October 2019, the Minister for Communications, Cyber Security and the Arts issued a spectrum re-allocation declaration to enable part of the 26 GHz band (25.1–27.5 GHz) to be re-allocated for spectrum licensing.[28] The ACMA is planning to allocate these spectrum licenses by auction in early 2021. The re-allocation is part of our broader plan to make spectrum available for 5G technologies in Australia through a mix of class, apparatus and spectrum licensing.[29] We are also implementing an area-wide apparatus licence (AWL) type, which could be used for novel IoT 5G purposes in the 26 and 28 GHz bands.[30]

Equipment standards

IoT devices are generally covered by the ACMA's existing equipment standards. Where an IoT device uses a telecommunications network to connect, the telecommunication standards would apply. Most IoT devices that use a non-telecommunications network to connect are covered by the Radiocommunications (Short Range Devices) Standard 2014, which covers devices ranging from Bluetooth devices and wi-fi routers to automatic door openers.

IoT is connecting new types of objects and devices. This change is also resulting in new types of devices transmitting radiofrequency emissions. This is expanding the radiocommunications regulatory footprint as new devices, market players and manufacturers will need to ensure these radiofrequency transmitting devices comply with the radiocommunications standards.

This growth of IoT devices in the Australian market has the potential to create regulatory and compliance challenges. We are mindful that this may result in new market players with no previous experience in complying with the radiocommunications standards entering the market. This may require us to adapt our approach to stakeholder engagement. We are also aware that new types of objects and devices transmitting radiofrequency could result in increased complexity in managing interference.

The increase in IoT devices and connections also poses potential challenges to interoperability. In February 2019, the International Standards Organisation (ISO) released the *Internet of Things: Interoperability for IoT systems* standard. The goal of the standard is to enable IoT systems to be built in such a way that entities in the IoT system can exchange information and mutually use the information in an efficient way.[31] This suggests that industry bodies are monitoring the issues around interoperability and adapting accordingly.

The security of IoT devices is an international issue. Australia, through the Department of Home Affairs, is working with likeminded international partners to develop a shared approach and implementation plan to improve IoT security globally.

---

[27] ACMA, *5G and mobile network developments; emerging issues occasional paper, February 2016, p. 3.*

[28] Radiocommunications (Spectrum Re-allocation — 26GHz Band) Declaration 2019.

[29] Department of Communications and the Arts, *Spectrum released for the 5G rollout,* 25 October 2019.

[30] ACMA, *ACMA approach to introducing area-wide licences*, February 2020, p. 6.

[31] ISO/IEC 21823-1:2019, *Internet of Things: Interoperability for IoT systems*, February 2019.

On 23 October 2019, Australia, Canada, New Zealand, the United Kingdom (UK) and the United States governments issued a statement of intent for IoT security. This statement of intent included a commitment to collaborate with industry and standards bodies to provide better protection to users by advocating that devices should be 'secured by design', and to raise awareness of security safeguards associated with IoT devices.

Several jurisdictions are looking at ways to improve the security of IoT devices. In February 2019, the European Standards Organisation (ETSI), launched the first globally applicable industry standard on internet-connected consumer devices, which specifies high-level provisions for the security of consumer devices connected to network infrastructure.[32] In May 2019, the UK Government launched a consultation on regulatory proposals to introduce new IoT security laws for manufacturers of connected devices aimed at ensuring IoT devices are better protected from cyber-attacks.[33] On 27 January 2020, the UK Government released its response to the consultation and announced plans to pursue a staged approach to regulation, starting with ensuring stronger security is built within consumer IoT products.[34]

In March 2020, the Cybersecurity Agency of Singapore introduced the Cybersecurity Labelling Scheme ('CLS') as part of Singapore's Safer Cyberspace Masterplan. The CLS was launched as a voluntary scheme and applies to consumer IoT. The scheme aims to differentiate smart devices with better cybersecurity provisions in the market, and to incentivise manufacturers and vendors to make products with improved safety features.[35]

Consumer safeguards

The ACMA considers there are unique privacy and security issues in relation to IoT. A significant challenge relates to consumer awareness and understanding of IoT functionality. IoT devices, like smart lights, wearables, smart toys, smart locks, and smart speakers, are transforming homes. According to the IoT Security Alliance, these devices are not always designed with security in mind, which may leave them at risk of malicious cyber activity.[36] The interconnection of these products may lead to increased safety risks to consumers through events such as malfunctioning software or cybersecurity breaches.

There is also an expectation from consumers that IoT devices available to them should be accessible, have security and safety principles (security by design), protections and processes embedded into their design, development, and deployment.[37] Manufacturers, retailers, suppliers, software developers, carrier and carriage service providers all play an important role in helping to protect consumers from security threats and that IoT devices meet minimum security standards.

Another key challenge is the new and complex supply arrangements and relationships in the IoT environment. While internet connectivity enables IoT applications, the relationships between consumers and IoT providers are usually separate from the

[32] ETSI, *Press release: ETSI releases first globally applicable standard for consumer IoT security*, February 2019.

[33] Department for Digital, Culture, Media & Sport, press release, *Plans announced to introduce new laws for internet connected devices*, May 2019.

[34] Department for Digital, Culture, Media & Sport, *Government response to the regulatory proposals for consumer Internet of Things (IoT) security consultation*, updated 3 February 2020.

[35] CSA Singapore, *Cybersecurity labelling scheme,* accessed 15 June 2020.

[36] IoT Security Alliance, *Demystifying IoT Security White Paper,* 2017 p. 2.

[37] Microsoft Azure, *New smart device consumer research: consumers call on manufacturers to do more*, 9 January 2019.

relationship between the consumer and their broadband service provider. This may create an information asymmetry for consumers due to the complexity of supply chains. It may also provide challenges for consumers seeking redress when a problem occurs, along with issues for industry in managing complaints about IoT services.

Importantly, there are a number of activities underway across the private sector and government that may help address these issues. For example:

- The proposed voluntary Code of Practice: Securing the Internet of Things for consumers, to be administered by the Department of Home Affairs, may address privacy and security issues associated with IoT. This proposed code of practice is a voluntary suite of measures that the Australian Government recommended for industry as the standard for IoT devices. The code of practice will also help raise awareness of security safeguards associated with IoT devices, build greater consumer confidence in IoT technology and allow Australia to reap the economic and social benefits of greater IoT adoption.
- The Australian Government's Response and Implementation Roadmap for the Digital Platforms Enquiry commits to ensuring privacy settings empower consumers and protects their data. The Implementation roadmap also outlines plans to implement an online privacy code and conduct a review of the *Privacy Act 1988*.
- The Australian Government's 2020 Cyber Security Strategy, administered by the Department of Home Affairs, is actively working towards developing stronger cyber defences to detect, deter and respond to cyber threats to encourage a cyber-smart nation.
- The Stay Smart Online Program funded by the Australian Government and delivered by the Australian Cyber Security Centre, provides easy to understand online security advice on various topics, including IoT.
- The ACMA notes initiatives by the IoT Alliance Australia to foster an industry self-regulatory response to potential security issues. This suggests a degree of alignment between industry and consumer interests that may help mitigate the risk of consumer harms arising from expansion of IoT.
- The ACCC's Product Safety Australia provides consumer information on interconnected devices, which includes buying tips for consumers, safety tips and publishes product safety recalls.
- The eSafety Commissioner provides safety tips for consumers on the safe use of wearable devices, including information on potential risks and tips on how to mitigate these risks
- The eSafety Commissioner has also developed Safety by Design (SbD) principles in 2019. SbD provide a model template for industry and places the safety and rights of users at the centre of the design, development and deployment of online products and services.

The ACMA will continue to monitor and evaluate any new vulnerabilities for consumers or industry resulting from IoT use in Australia. How IoT is interacting with the current consumer safeguards, such as interoperability of network devices, access to emergency services, privacy, and health and safety requirements is also being monitored. These issues may be heightened as IoT devices are increasingly adopted by a broader range of consumers.

***IoT bytes*—Digital literacy**

While IoT delivers significant benefits to consumers, it is also posing unique challenges. IoT devices change the concept of a physical object being in the complete control of the individual, as the device connects to the digital world. This creates new challenges such as privacy, security and safety.

Vulnerabilities in a connected device could potentially compromise an entire home network. IoT devices may have insecure default passwords, which may leave them vulnerable to cyber-attacks. The scale of data collected by IoT devices, when analysed alongside other information, could reveal personal information and preferences, which may pose difficulties for consumers in managing their data privacy. While there is work being done to enable industry to address these concerns (such as the proposed IoT code of practice), consumers may need to be supported in understanding these issues, and actions taken by industry to address them. Improved digital literacy for consumers could also help address this information asymmetry.

The ACMA will continue its work with government, industry and consumer groups to consider and implement suitable regulation for the industry. This could take the form of retaining existing regulation to further enable Australian businesses and consumers to benefit from IoT, or, over the long-term, introduce new regulation related to the connectivity of IoT devices, the data captured and the security standards of the devices themselves, if current arrangements prove to be no longer fit for purpose.

Regulatory settings and supportive tools for IoT

IoT has, in general, been successfully encompassed within the ACMA's current media and communications regulatory arrangements. This is evidenced by market growth in IoT, along with the growth in Australian households adopting this technology. Our current settings appear to be well-suited to deal with the immediate issues identified in this paper that are within our remit.

However, as the IoT market continues to expand within Australia and evolve in new ways, unforeseen regulatory issues may emerge. We will continue to monitor IoT developments and outcomes to ensure our regulatory settings remain fit for purpose.

IoT bytes—Adapting regulatory settings to IoT below provides examples of how we have readjusted our regulatory settings to accommodate IoT.

***IoT bytes*—Adapting regulatory settings to IoT**

The Radiocommunications (Communication with Space Object) Class Licence 2015 authorises the operation of earth stations that communicate with apparatus-licensed space stations on authorised frequencies. In November 2018, this class licence was varied to include spectrum around 400 MHz, which enabled satellite operators to implement direct-to-orbit satellite IoT.

As outlined in our *Corporate plan 2018–19*, we are already assisting stakeholders in preparing for autonomous vehicles, and the anticipated developments in M2M communications associated with IoT, which promise to transform multiple, diverse sectors of the economy.

Looking ahead, we will continue working with industry groups, government, and other regulators to gather feedback on whether our regulatory settings will require adjustment to support the ongoing development and effective implementation of IoT. This could take the form of amendments to existing regulation to facilitate and support consumers and industry to benefit from IoT. Consumer education on the data captured by IoT devices, and the security standards of the devices themselves, may also be required.

We will continue to review whether our regulatory settings and tools are supporting enduring public policy objectives. The ACMA's previous analysis on IoT identified enduring concepts of most relevance to IoT[38], including:

- **national interest**—regulatory settings should reflect the national interest both domestically and through international fora (for example, radiocommunications planning is governed by treaty)
- **competition and efficiency**—markets should be open and competitive to encourage investment, innovation and diversity of choice; policy settings should be coherent, appropriately calibrated, and predictable so that a minimum level of service is available to all and public resources are used efficiently over time

[38] ACMA, *The Internet of Things and the ACMA's areas of focus, emerging issues in media and communications occasional paper*, November 2015, pp. 25–6.

- **access to services**—citizens should enjoy reasonable and equitable access to communications infrastructure, services, and the content necessary to promote their effective participation in society and the economy
- **values and safeguards**—services should reflect community standards, meet community needs and be 'fit for purpose'; users should be provided with effective and accessible avenues of complaint and redress if standards are not met.

ACMA IoT planned activities

ACMA activities already underway to support the continued development of IoT in Australia include:

- monitoring of spectrum demand drivers, including IoT
- planning and allocation activities in accordance with the ACMA's 2020–21 annual spectrum management work program
- reviewing, and as appropriate, updating licensing arrangements to support IoT as required, including the area-wide apparatus licence (AWL) type
- collating data on IoT use and consumer awareness through the annual consumer survey as a part of our 2019–20 research program
- working with international standards bodies to promote and protect Australian interests.

Over the medium- to longer-term, we will continue to:

- monitor standards developments through international fora
- review our regulatory settings to ensure Australia's IoT environment is adequately supported
- undertake research that examines IoT take up and usage trends, and which considers how current and future developments in the communications and media landscape will impact public interest outcomes and our role in regulating communications and media, including IoT
- monitor developments and work with stakeholders, including industry, consumer groups, regulators and equipment vendors.

Figure 5 summarises these activities.

Figure 5: The ACMA's planned IoT activities