THE INTERNET OF THINGS

EXTRACT

Full report available at
www.acola.org

HORIZON SCANNING

ACOLA
AUSTRALIAN COUNCIL OF LEARNED ACADEMIES

EXPERT WORKING GROUP

Professor Bronwyn Fox FTSE (Chair)
Professor Gerard Goggin FAHA
Professor Deborah Lupton FASSA
Professor Holger Regenbrecht
Professor Paul Scuffham FAHMS
Professor Branka Vucetic FAA FTSE

AUTHORS

Professor Bronwyn Fox FTSE (Chair)
Professor Gerard Goggin FAHA
Professor Deborah Lupton FASSA
Professor Holger Regenbrecht
Professor Paul Scuffham FAHMS
Professor Branka Vucetic FAA FTSE

Supported by Stephanie Chan, Ella Relf, Dr Lauren Palmer, Ryan Winn and the generous contributions of many experts throughout Australia and New Zealand. A full list of contributors can be found in the written submissions section of the full report.

PROJECT MANAGEMENT

Stephanie Chan
Dr Lauren Palmer
Ryan Winn

© Australian Council of Learned Academies (ACOLA)

ISBN 978-0-6483303-8-7 (print)
ISBN 978-0-6483303-9-4 (digital)

This work is copyright. All material published or otherwise created by the Australian Council of Learned Academies (ACOLA) is licensed under a Creative Commons – Attribution – Non-Commercial 4.0 International (CC BY-NC 4.0) licence.

DATE OF PUBLICATION

November 2020

PUBLISHER

Australian Council of Learned Academies
Level 6, 436 St Kilda Road
Melbourne Victoria 3004 Australia
Telephone: +61 (0)3 9864 0923
www.acola.org

REPORT DESIGN

Lyrebird
jo@lyrebirddesign.com

SUGGESTED CITATION

Fox, B., Goggin, G., Lupton, D., Regenbrecht, H., Scuffham, P., Vucetic, B., (2020) *The Internet of Things*. Report for the Australian Council of Learned Academies, www.acola.org.

ACKNOWLEDGEMENT OF COUNTRY

ACOLA acknowledges the Traditional Owners and custodians of the lands on which our company is located and where we conduct our business. We pay our respects to Elders past, present and emerging.

ACOLA
AUSTRALIAN COUNCIL OF LEARNED ACADEMIES

By providing a forum that brings together great minds, broad perspectives and knowledge, ACOLA is the nexus for true interdisciplinary cooperation to develop integrated problem solving and cutting edge thinking on key issues for the benefit of Australia.

www.acola.org

Working together

The Australian Council of Learned Academies (ACOLA) combines the strengths of the Australian Learned Academies.

LEARNED ACADEMIES

ACADEMY OF THE SOCIAL SCIENCES IN AUSTRALIA

Australian Academy of Science

Australian Academy of the Humanities

ATSE Australian Academy of Technology & Engineering

ASSOCIATE MEMBER

Australian Academy *of* Health and Medical Sciences

ACOLA receives funding from the Australian Government Department of Education, Skills and Employment.

HORIZON SCANNING SERIES

We live in a time of rapid change – change that is driven by developments in science and technology and challenged by our capacity to adapt in the present and prepare for the future.

Commissioned by Australia's Chief Scientist, on behalf of the National Science and Technology Council, Horizon Scanning reports present independent and timely analyses to guide decision-makers through the decade ahead.

Horizon Scanning reports by the Australian Council of Learned Academies (ACOLA) draw on the deep disciplinary expertise from within Australia's Learned Academies to analyse the future, navigate change and highlight opportunities for the nation. As interdisciplinary studies, ACOLA's reports include economic, social, cultural and environmental perspectives to provide well-considered findings that inform complete policy responses to significant scientific and technological change.

This project has been supported by the Australian Government through the Australian Research Council (project number CS170100007) and the Department of Infrastructure, Transport, Regional Development and Communications.

ACOLA collaborates with the Australian Academy of Health and Medical Sciences and the New Zealand Royal Society Te Apārangi to deliver the interdisciplinary Horizon Scanning reports to government.

Also in the Horizon Scanning Series

The role of energy storage in Australia's future energy supply mix
Published 2017

The future of precision medicine in Australia
Published 2018

Synthetic biology in Australia: an outlook to 2030
Published 2018

The effective and ethical development of artificial intelligence: an opportunity to improve our wellbeing
Published 2019

The future of agricultural technologies
Published 2020

PROJECT AIMS

1. Examine the impact the IoT is likely to exert on Australia over the coming decade.
2. Identify and assess the opportunities and challenges presented by the deployment of the IoT in Australia, both in key industry sectors and as an economy-wide enabler, including:
   - the scientific, technological, economic, security, social, privacy, data ownership, regulatory and other impacts of the different IoT technologies, applications, data and users
   - the future education, workforce, regulatory and infrastructure requirements to support the practical measures governments, industry and other stakeholders could consider to maximise the benefits of IoT deployment and mitigate potential harms.
3. Explore the interrelation of IoT systems, people and the underlying infrastructure (e.g. communication systems, transportation) that is essential to modern life.

KEY FACTS ABOUT THE IOT

Infrastructure Australia estimates that there will be **29 billion connected devices in the world by 2022** of which around 18 billion will be related to the IoT.

The Bureau of Communications and Arts Research has estimated that **IoT activity increased by**

$10.5 billion

or 16.5 percent from $63.8 billion in 2012-13 to $74.3 billion in 2016-17.

Strong and ongoing community engagement will be needed to maximise the benefits of IoT-enabled technologies.

One of the biggest security challenges with IoT systems is the substantial **increase in the number of available surfaces for security attack**.

A mixture of **hard skills**, such as coding, maths and physics, and **soft skills**, such as communication, collaboration, creativity and problem solving, are likely to be required for future careers in the IoT and related technologies.

It is estimated that by 2050 the IoT could consume between **one and five percent of the world's electricity**.

Smart IoT techniques will **monitor speed, detect real-time incidents and provide real-time warnings** to inform drivers and road agencies of any hazardous situations on the road.

IoT is likely to create jobs in network design, planning and implementation, cyber-security, energy management, and data monitoring, management and analysis.

IoT applications are likely to exist on a **4G and 5G hybrid network in the next two to four years**. Standalone 5G networks (requiring core architecture) are not likely to emerge until around 2025.

CHAIR'S NOTE

The Internet of Things (IoT) can be described as a distributed measurement and control system with sensors and real-time analytics that utilises the internet to enable applications. While the term 'the Internet of Things' was coined over two decades ago, it is only in the past few years that rapid developments in sensor and communications technologies, artificial intelligence (AI) and edge computing have revolutionised the way we envision networked IoT systems and possible applications. Australia has a moment in time to capture the benefit of these combined advances in IoT to develop unique applications, or we risk losing our competitive advantages and being excluded from global value chains.

New advances in telecommunications such as 5G mean that devices can now be connected in wider, denser ecosystems. AI-driven analytics and edge computing (where the analytics are done at or near the source of data) have also changed the computational output of these devices: they are smaller, lower-powered and cheaper but powerful enough to work at the 'edge' of a network and make determinations based on real-time data gathered from the external environment. While devices have been smart and connected for some time, they are increasingly becoming more *pervasive* and *knowing*, with the ability to make decisions on our behalf. This is already occurring in our everyday lives: smart traffic light systems are deciding which vehicles go first on a congested motorway or determining when a home swimming pool should be cleaned based on daily electricity rates.

As of August 2020, the COVID-19 pandemic has meant that society as a whole has embraced digital technologies. It has also made us consider the importance of accurate and timely data collection. The IoT offers a high level of visibility into the systems and processes we use. This could improve our decision making so that decisions and outcomes are based on evidence, rather than limited knowledge or assumptions that we may have previously relied on. For example, remote monitoring of infectious COVID-19 patients with mild symptoms has been piloted in Australia through IoT-enabled pulse oximeters and a combination of AI and medical staff observations. The ability to monitor patients safely at home provided an opportunity to reduce pressure on the hospital system. When a monitored patient's symptoms worsened, an IoT system immediately called an ambulance to the patient's home address.

The devastating impacts of the recent bushfire crisis also highlighted how critical digital technologies are helping us to respond safely to environmental disasters. Many regional communities relied on a mobile platform that

consolidated publicly reported data to obtain up-to-date information about where fire fronts were located and when community members needed to evacuate. IoT sensor networks combined with AI-driven analytics could further enhance these types of initiatives. For example, they could provide accurate real-time data to produce topographical models of bushfire risk in high-risk areas, model pathways for escape and even calculate the expected economic risks. A review by the Australian Communications and Media Authority found that a total of 1,390 facilities were directly and indirectly impacted by the bushfires. Of all the facilities impacted, 51 percent experienced outages of four hours or more. The bushfire season demonstrated our growing dependence on reliable connectivity and telecommunications infrastructure, as many essential services now depend on connectivity. While this may not be an issue in urban areas, there may be a disproportionate impact on rural, regional and remote communities (RRR). Multimodal communications solutions, where redundancies are factored in, need to be considered.

Given the pace of innovation, it is fascinating to imagine where we will be in ten years time. The IoT will create economic impact for Australia, present novel opportunities for the ways we live and conduct business, and provide solutions to societal issues such as environmental disasters and pandemic management. The applicability of the IoT across all sectors is enormous. It is predicted that within the next decade, we will see advances in IoT-enabled smart mobility – from connected autonomous vehicles (CAVs) to improve road safety and convenience, to the use of 'mobility as a service' (MaaS), which will provide the ability to plan our daily commute using all modes of travel (such as bike, car, ferry and tram) through a single digital platform based on time, cost and convenience. There will undoubtedly be a further revolution in IoT-enabled health outcomes, with health wearables providing real-time health data to enhance patient-centred care, not only in hospitals but also in homes. The IoT will also create a new paradigm in manufacturing, using flexible, self-correcting manufacturing processes to create cost-effective bespoke products. This could catalyse a manufacturing renaissance in Australia over the next decade, allowing the design and construction of many products that are currently manufactured overseas to be re-shored. In particular, ultra-reliable low-latency communications (URLLC) shows great promise to support latency-sensitive applications including industrial automation, connected and autonomous vehicles and tele-surgery.

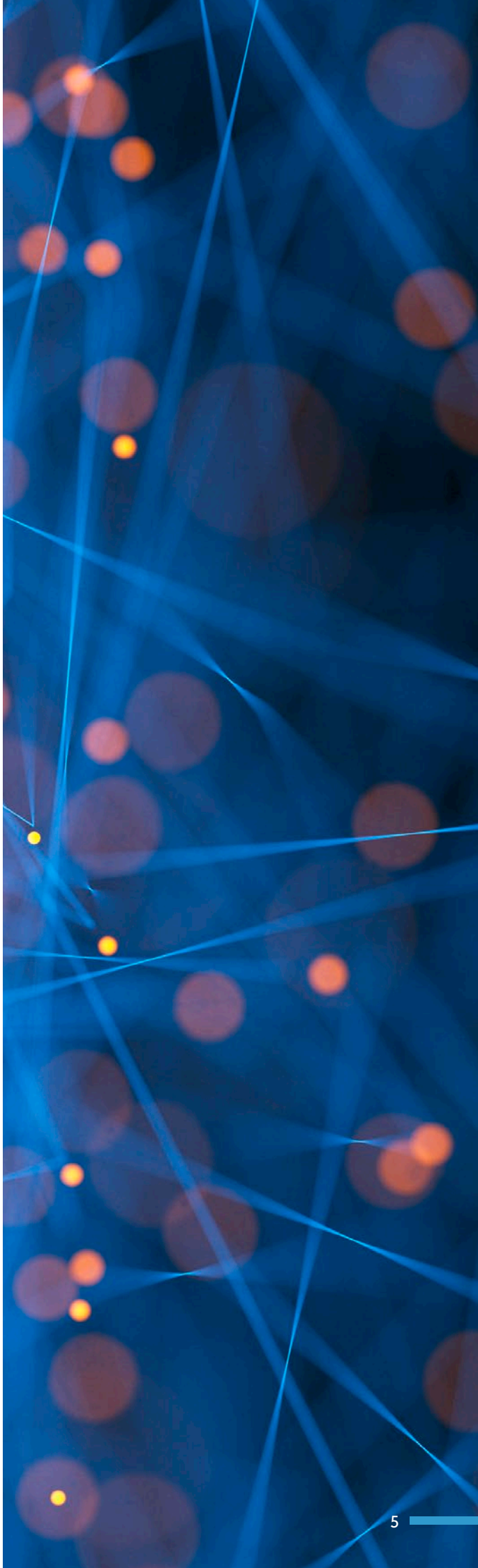
However, the advances mentioned above, AI-driven analytics, 5G telecommunications and edge computing, will fundamentally change the way that the IoT is used in society. The pervasiveness of these systems and the degree of granularity of the data collected is raising new levels of concern about privacy and data sovereignty. An important theme in this report is digital trust creation. This is likely to be an ongoing balancing act. Government, society and industry will need to continually reassess values such as privacy, optimisation and convenience and consider which are more important and whether there are trade-offs that need to be made. Frameworks that set minimum standards of protection, together with ongoing community engagement and education, will help to build the trust and acceptance that will be needed to maximise the opportunities that the IoT presents.

Sustainability is another key issue that will require consideration over the next decade. While IoT devices and systems offer benefits, the energy to power these systems is likely to require one to five percent of the world's electricity by 2050. As our report demonstrates, there may even be rebound effects, where there is *increased* energy consumption using these devices to enable enhanced comfort, convenience, security and entertainment. It is therefore important to consider how sustainability can be integrated into the design of IoT devices and systems at the outset.

While many recent reports have predicted the future economic impact of the IoT, the pervasiveness of this technology means that this is very complex to estimate, however we do know that the benefits to society and the economy are likely to be substantial. We have identified a number of technological fields where Australia has a unique advantage and highlighted emerging trends where, if we do not keep up, we risk losing global competitiveness.

I would like to thank each individual member of the Expert Working Group who volunteered their time to contribute to this report and the talented team at ACOLA. Thank you also to the people who made valued contributions through our consultation process with government, industry, academia and community, focusing on the real-world issues related to the IoT that Australia is well placed to solve. My personal thanks also to all of the incredible experts from around the world who contributed their thoughts and reviewed the document.

Professor Bronwyn Fox FTSE



EXECUTIVE SUMMARY

The IoT can be understood as a distributed measurement and control system, connecting smart objects, devices, networks and platforms, that collects, processes and analyses real-time data to enable a broad range of applications and functions. Recent advances in IoT enabling technologies such as 5G, edge computing and low powered artificial intelligence have elevated the urgency to embrace IoT platforms for Australia to remain globally competitive.

IoT devices and applications have far-reaching uses and benefits, some of which present novel opportunities. These are achieved through devices and systems that enable:

- locational awareness
- environmental awareness
- medical monitoring
- industrial monitoring
- real-time remote operation of assets
- operation at continental scale.

The IoT already exists in a nascent form; however, rapid developments in wireless connectivity, miniaturisation and advances in AI will enable the IoT to become embedded into the fabric of our society, much like the conventional Internet. The opportunity is vast, but there are also risks, including: not mitigating the harms or unintended consequences of the IoT, or being unprepared to capitalise on this technology.

What does the term 'Internet of Things' actually mean?

The IoT is a gigantic network of connected smart 'things', enabled by data analytics and artificial intelligence, that can make our lives easier, cheaper and more reliable. Examples of these include home devices, health wearables, agricultural sensors, and autonomous factories and mines.

Over the next decade, IoT capabilities will increasingly become embedded into services and products. The capture of exponentially increasing volumes of granular data will enable us to analyse patterns, anticipate changes and alter objects and the surrounding environment. The data will also help us to optimise the services and products that generated the data and will drive future innovation and research. A critical aspect of IoT development over this period will be

advances in data analytics and AI to expand human-to-machine or machine-to-machine (M2M) interactions and edge computing. Devices are increasingly smaller, lower-powered and have the computational output to make decisions at the edge of the network. Potential benefits are multifactorial, with the opportunity to improve processes and systems across society – within the home, across industries and in public service delivery.

To capitalise on this opportunity, Australia must look to niche areas of strength or comparative advantage. For example, advanced manufacturing (where the application of Industrial IoT is known as Industry 4.0[1]) and the health sector are already beginning to understand and use the IoT to increase productivity and reduce costs. Australia should also consider leveraging its unique geographic diversity, climate and dispersed population as a testbed for future applications.

The Australian and state and territory governments are already progressing a range of initiatives that will help support Australia's transition towards a digital economy, both in managing the technologies and preparing the workforce. Many of these lay the foundation for supporting the effective implementation of the IoT, as well as other emerging digital technologies, such as AI and blockchain. Further actions will be needed that address the specific needs of the IoT and emerging technologies in general, to ensure that its continued adoption is smooth, cost effective and supports responsible and ethical usage, especially in the areas of data privacy and cybersecurity.

We have had sensors for a long time, how and why is IoT a game changer now?

A number of technological advances have allowed connected objects to become intelligent: 'sensing and knowing'. This enables them to communicate and make decisions in real-time without or with less human input. There are diverse opportunities to apply this technology to which can the way our society functions.

1 Initially coined by the German government, Industry 4.0 refers to the fourth industrial revolution, where advances in automation and digitisation technologies in manufacturing, such as IoT, cyber–physical systems and big data analytics, are enabling a higher level of operational productivity and efficiency.

Opportunities and challenges

Cities and regions

There are opportunities to promote the development of smart cities and regions through the measured introduction of IoT technologies. In cities, current and potential benefits include: (i) energy use, such as rooftop home solar installations connecting to the national electricity market to manage energy consumption and resale of excess stored energy; (ii) enhanced citizen and government engagement, such as using IoT sensing ecosystems and mobile apps to provide real-time information on weather and public transport; (iii) improvements to service delivery, such as smart lighting and smart bins to enhance the use of public spaces and buildings; (iv) healthcare, using wearables such as insulin monitors to manage remote patient care; (v) enhancing student experiences education by monitoring facilities and services such as the use of shared study areas.

In RRR areas, benefits include (i) cost savings and efficiencies in agriculture and resource use, for example monitoring environmental conditions such as soil moisture to improve crop growth; (ii) improved quality of and access to healthcare, for example using IoT wearables to enhance patient-centred care, which is currently limited by distance and cost; (iii) enhancing education experiences, for example by enabling access to data from IoT systems in urban-located facilities such as research labs to support distance learning and research; and (iv) disaster and emergency management, such as monitoring environmental conditions to prevent and manage bushfires and drought.

Challenges include assessing connectivity and access, as well as identifying potential risks and unintended consequences that may occur with the uptake of an emerging technology. For example, while industry tends to highlight the energy-saving benefits of IoT technologies, research has demonstrated that usage may in fact increase overall energy consumption in households due to factors such as increased convenience, known as rebound effects. Energy efficiency strategies may not be sufficient and could be complemented by sufficiency strategies[2] and evaluations of energy consumption by IoT in practice, as well as community education and awareness raising.

The environmental and sustainability impacts of the manufacture and usage of IoT devices are also likely to be substantial. Growing dependence on devices to support our digitally enhanced lifestyles is likely to lead to the exponential growth of e-waste, arising from virtual wear-out, planned obsolescence or vendor lock-in. Holistic and sustainable design approaches will be important for industry and government to consider as ways to mitigate these risks.

Security

Security vulnerabilities will be an ongoing challenge as IoT applications become more ubiquitous over the coming decade. Australia should continue to be proactive in its approach to security to ensure that minimum baseline protections and redress mechanisms meet citizen expectations. Australia's ongoing

2 This is a sustainability strategy that aims to limit or reduce the demand for energy supplied by technology through changes in technology use and other use aspects to a sustainable level.

participation in international standards committees will continue to play an important role in monitoring and managing national privacy and security interests as well. Care should also be taken when sourcing IoT devices or components from countries with poor security and privacy track records. Governments could provide leadership in protecting personal data and helping Australians to be aware of and understand security risks associated with IoT technologies.

Privacy and data

It is likely that a greater quantity of data, including personal or sensitive data, will be collected and processed by industry. However, users' knowledge of what and how much data are being collected and by whom, the uses of that data and how long data are used may be limited. Ensuring that legislative measures in Australia are cohesive and adequate at establishing a baseline of protection and responsibility is a key consideration for the Australian Government. National data standards that build on the ongoing work of the Office of the National Data Commissioner (ONDC) could provide guidance on the definition, capture, analysis and reconciliation of data across all three levels of government. It will be important for governments and industry to consider the usability, availability, security, integrity and commercialisation of data as IoT applications extend into diverse industry and public service contexts and supply chains over the next decade.

Standards and interoperability

International IoT standards are currently heterogenous, and consolidation over the next decade will increase the likelihood of effective implementation internationally and domestically. There is growing recognition for the need for collaboration through international forums and standards-making bodies to provide both international guidance to industries and countries. Australia's continued participation in international standards committees will be important to manage our interests and monitor international developments. Building on existing frameworks and national and international regulations on data security and privacy, our domestic approach to standards should continue to focus on being technology-neutral, flexible and principles-based. With this approach, Australia could be a model for other countries seeking to develop the IoT in a measured and responsible manner.

The mobility sector may face specific challenges with interoperability due to manufacturing mostly occurring overseas. Consistent regulations across states and territories will reduce industry uncertainty and prevent barriers to the deployment of CAVs, particularly by overseas manufacturers, given Australia's relatively small market size.

Social and community considerations

Across Australia and internationally, communities are at relatively early stages in their engagement with the IoT. It is still unclear how the IoT will interact with social change factors in the Australian context. Research is required on the social and cultural dimensions of IoT use across the broad range of potential domains in Australia, including farming, education, healthcare, transport and industry, as well as consumer IoT devices. Current knowledge gaps include how Australians across these domains understand what is meant by the IoT, what benefits they gain from these technologies, factors that might affect their use or avoidance of the IoT and what developments and improvements would help the IoT to better suit their needs. In addition, it would be beneficial to assess

the potential for the IoT to exacerbate existing inequalities or create new impacts or harms, such as the impact on the elderly or children, Indigenous communities or those who may choose to opt out of this technology.

Proactive stakeholder engagement and alignment with community values will be integral to building trust and demonstrating the value of IoT initiatives and products to Australians.

Jobs, training and research

The inter-connected nature of the IoT and related technologies, such as Industry 4.0, block-chain and machine learning, is expected to have compounding effects, impacting the job market more significantly than through the independent use of these technologies. The expected digital disruption and complexity of the IoT is therefore likely to require the development of both 'hard' technical skills and 'soft' non-technical skills over the next decade.

A domestic IoT industry is likely to create jobs in network design, planning and implementation, cybersecurity, energy management, and data monitoring, management and analysis. Other potential areas include Industry 4.0, and sensor and systems design and management. To meet these needs, Australian universities have begun to offer IoT-specific subjects and degrees. This is likely to provide new opportunities in international education to support a domestic and international workforce, building on Australia's existing global reputation for high quality education.

As jobs evolve over the next decade, businesses and government could actively assess opportunities to promote the importance of continuous learning, in order to skill, re-skill and upskill workers. Targeted up-skilling programs and innovative learning methods, including augmented reality (AR)-based training, game-based learning and micro-credentials, may help bridge skill shortages. Support may be required for small to medium enterprises (SMEs) to upskill their workforce.

Important enablers to support an IoT-capable workforce include partnerships between industry, education and employers to facilitate access to industry-relevant training, as well as the necessary cloud and network infrastructure for student learning. It will also be important to future-proof the national curriculum to ensure that students have a mixture of hard and soft skills. Trainers and teachers at all levels will need to up-skill and acquire the necessary knowledge to equip students for the changing workforce, with government and industry playing a crucial part in this process.

If the IoT becomes ubiquitous across Australia, it may provide new opportunities for employment and education in RRR areas. For example, increasing requirements for the storage, hosting and security of data have led to the establishment of data centres in RRR areas, which may lead to the creation of jobs in cloud and hosted services. To support education and the creation of IoT jobs, ongoing institution-wide commitment and collaboration between vocational education and training (VET) providers, universities, external agencies and community networks will be needed.

Areas for future research include new and novel IoT applications; the number of devices in Australia; the economic value of data, with particular respect to the shifting boundaries of property rights regimes; social impacts of IoT across homes; smart cities and RRR areas; future environmental impacts of devices; the use of CAVs; and ongoing research into the use of radiofrequency electromagnetic energy (RF EME) and 5G to reassure the Australian public.

National approach

This report outlines a range of opportunities and challenges, as well as practical actions and measures that Australia could consider in the deployment of IoT responsibly and effectively in our cities and regions. However, the inherent complexity and breadth of this technology necessitates a national approach to highlight areas where Australia could prioritise its efforts. This would identify and galvanise areas for individual and collective action by government, industry and community. In addition, a national approach would be useful to articulate the potential risks that the IoT poses, as well as the strategies to minimise harms and unintended consequences. This would help build community trust and acceptance and encourage industry to take a considered and measured approach in developing IoT. Engagement and collaboration across community, industry and government is likely to be required. As outlined in the key findings of the report, some areas that could be considered in a national approach are:

- ensuring that Australia has flexible, technology-neutral, principles-based regulatory settings
- establishing minimum safeguards for the digitally illiterate or ambivalent, including open data frameworks, privacy and consumer protection policies, and baseline security measures
- incentivising research and development (R&D) of IoT technologies, particularly in niche areas where Australia has existing capabilities
- engagement of citizens and consumers in the design and development of IoT systems and their implementation
- building early community awareness, trust and acceptance of IoT technologies
- ensuring the necessary connectivity across our cities and regions to enable the use of the IoT
- identifying and supporting initiatives that future-proof our national curriculum, and building capabilities and expertise to create a domestic IoT sector.

By taking a national approach we will be able to realise the potential of this extraordinary but currently poorly understood technology that in time will redefine our society and economy. A proactive approach to adoption will allow Australia to remain globally competitive in the rapidly evolving digital landscape over the next decade.

KEY FINDINGS

1 National focus and strategy

2 Australian advantage

3 Smart cities and regions

4 Data use and privacy

5 Flexible frameworks

6 Security

7 Public acceptance and education

8 Economic growth, skills and training

9 Research and emerging technology

1

Australia could consider a national approach on IoT, with a view to responding to the opportunities and challenges that IoT present over the next decade, building on existing industry and government efforts.

- A national approach to the IoT developed collaboratively by industry, governments, academia and the community will support the ethical, efficient and effective deployment of the IoT in our cities, regions and society. This would provide guidance on some of the key use cases that will be beneficial to Australia.
- At a minimum, it could identify the expectations for regulations, standards, connectivity, and future research and investment priorities.

2

Australia should focus on areas of strength and comparative advantage to bolster our competitiveness in the global IoT market. This includes leveraging our geographic and climate diversity to test novel IoT applications.

- Over the next five years, industry should focus on developing niche IoT solutions where it has specific expertise or global scale, for example in agriculture, resource management, environmental monitoring, disaster management, health, mining and mass data collection in smart cities or regions.
- Opportunities for niche products or services in these sectors include:
  - tailored middleware solutions for industry verticals (i.e. where products can only be used in one particular industry, for example, the health industry)
  - platform solutions that can be integrated with existing platforms used across horizontal markets (i.e. where developed products can be used by customers regardless of industry)
  - leveraging unlicensed spectrum to provide connectivity solutions in niche areas, such as rural, regional or remote areas.
- IoT-enabled solutions will facilitate the development of a competitive advanced manufacturing sector (Industry 4.0) in Australia over the next 10 years. Key focus areas include developing capabilities in digital twin technology and automation.

- The recent investment and focus on space technologies could be leveraged by the IoT satellite and telecommunications sector to build scale in the domestic industry and encourage research and collaboration.
- Although 5G is still an emerging technology in Australia and is likely to remain so until 2025, industry and governments could consider the next iteration of wireless technologies, tentatively characterised as 6G, and its role in future connectivity in Australia. Participation by industry and the Australian Government in international forums to shape the global conversation and consider opportunities for national deployment would be beneficial.
- Translation from research to commercialisation is an ongoing challenge for emerging technologies. Government, industry and academia could canvas existing partnerships to encourage the ongoing development of IoT products and services over the next decade. Industry could include humanities and social sciences researchers in IoT R&D to assess the social and ethical concerns of commercial products.
- The integration of IoT technology into service delivery by governments should be considered in the broader reinvention of governance and government as a service.

3

Opportunities to implement the IoT to improve wellbeing and quality of life in Australian cities and regions will enable greater understanding of the technology and its applications by government, businesses and communities.

- Benefits to the development of smart cities through the considered introduction of IoT technologies include: optimising energy production and use, waste management, service delivery (e.g. health, public transport, and public spaces and buildings) and education, reducing road congestion, and enhancing citizen and government engagement.
- Benefits to regions include promoting cost savings and efficiencies in agriculture and resource management, enhancing disaster management, and improving the quality of and access to healthcare.
- Given governments' significant investment in past and current IoT initiatives in cities and regions, there could be a greater role for the Australian Government to facilitate:
  - the sharing of learnings and international best practice with and between, states and local governments to assess broader impact and scalability
  - collaborations between industry, academia, governments and communities in identifying and implementing potential solutions
  - identification of IoT systems that will be of greatest use and ongoing cost-benefit to communities

  - understanding and mitigating the risks of smart system failures and security breaches to mitigate the scale of potential impacts and harms
  - understanding of the impacts of increasing dependence on major technology companies and the potential merging of private and public interests in the provision of service delivery.
- The Australian Government could continue to explore different connectivity solutions for RRR areas, so that these communities can access the benefits of IoT technologies.
- Data captured from IoT applications could be used to measure at a national level the comparative performance of cities and regions in indicators such as sustainability, quality of service delivery and population mobility. These data could be used to inform inputs and metrics such as the National Cities Performance Framework.

4

Digitalisation is expected to continue at a rapid pace over the next decade. It is important to ensure that data collection, usage and application from the IoT and related digital technologies is ethical, meaningful and fit for purpose, supported by appropriate legislation and regulatory frameworks.

- Building on existing initiatives, the Australian Government could provide leadership in developing national data standards relating to the definition, capture, analysis and reconciliation of data, to ensure that data are appropriately used and shared.
- As the value of data grows, the Australian Government could regulate the ownership, usability, security, integrity and commercialisation of data by industry, particularly where there may be new asymmetries in data access and re-use by major platform companies, compared to smaller Australian companies and citizen initiatives.
- All levels of government could consider the use of application program interfaces (APIs), data marketplaces and data collaboratives or 'trusts' that seek to create common protocols and frameworks for data sharing across vendors, public–private agencies and citizens.
- The IoT will create challenges for existing legislative measures in Australia, which may test whether existing privacy and cybersecurity frameworks are fit for purpose. Areas that may require ongoing review include:
  - building on forthcoming review of the *Privacy Act 1988 (Cth)* and the potential impacts of the IoT on businesses and consumers
  - considering the functions and ongoing resourcing of the Office of the Australian Information Commissioner and the Office of the National Data Commissioner to meet consumer and industry expectations related to the IoT
  - assessing the applicability of current definitions of technology-facilitated abuse and other criminal acts to ensure they cover the scale of IoT applications.

5

Regulatory frameworks and policy guidelines should be technology-neutral, flexible and principles-based building on existing frameworks. This will ensure they are consistent with international standards, and can respond to future technological developments and changing consumer behaviours and preferences over the next decade.

- Current international standards represent the range of interests of device manufacturers, service providers, governments and standards-making bodies. Over the next decade, standards will continue to be driven by international developments. The Australian Government and industry bodies could continue to participate in global forums to understand these developments and to ensure national interests are supported and represented.
- The development of any national standards by the Australian Government or industry should be principles-based to ensure that Australia is able to fully participate in global supply chains. Public engagement on these standards will be an essential part of this process.
- Consistent regulations across states and territories will reduce industry uncertainty and prevent barriers to the deployment of CAVs, particularly by overseas manufacturers, given Australia's relatively small market size.
- The Australian Government could continue to assess Australia's transition towards a distributed energy system. Standards should be considered to regulate data use and collection by consumers, ensure that local incumbents do not slow down adoption, and to ensure that localised smart grid infrastructure is reliable and safe to support these new models.

6

Australia should continue to be proactive in its approach to security and could establish baseline protection and redress mechanisms. These will need to be adapted as the digital landscape evolves and new risks arise, including in the context of increased IoT adoption and deployment.

- The Australian Government could establish baseline security standards for the use of IoT technologies in government agencies to protect citizen data. Best practice standards would provide leadership and guidance to state and territory and local governments.
- Australia should continue to monitor international developments relating to security. Governments and industry should be cautious when procuring technology solutions from overseas companies and nations that may have competing security interests.

- Security measures on the use of IoT technology must be proactively assessed by government, businesses and consumers. Consideration could be given to:
  - assessment of supply chains to ensure an appropriate level of independent testing and protection against unauthorised access, control or interference
  - creating security guidelines and policies that are agile enough to be applicable to future technologies
  - certification of whole systems, not just components and products
  - considering software resilience and redundancy
  - robust end-to-end system maintenance.

7

Early and proactive community education and engagement is necessary to encourage community awareness, acceptance and trust of the IoT and related digital technologies, particularly as IoT devices and applications become more widespread and embedded in our built environment.

- Educating the public about data-collection techniques and security vulnerabilities in devices and infrastructure is vital. This includes how data are used in data-driven services in everyday life (e.g. public transport and infrastructure), informed consent for data collection, and choices about devices, manufacturers and service providers.
- Potential harms of the IoT go beyond privacy and security and include threats to personal safety, health and wellbeing. Ongoing government and community-led engagement on the potential risks and harms of the IoT is important, particularly for vulnerable groups, including children and socioeconomically marginalised and disadvantaged people.
- Government and industry could refine existing tools (e.g. developing privacy, ethical and social impact assessments) to assist designers and innovators with self-assessing their IoT technologies during development to support user-centred design.
- Participatory citizen-sensing initiatives in galleries, libraries and museums may assist in improving data literacy and creating better community awareness and understanding of IoT applications.

8

Close industry–government–education collaborations will help to ensure that Australia's workforce acquires the new skills and enhanced capabilities necessary to thrive in an IoT-permeated economy.

- The IoT is likely to require both 'hard' technical skills (e.g. IoT engineering, cybersecurity, data science and data knowledge) and 'soft' non-technical skills (e.g. user-centric design, critical analysis of social issues, problem solving and ethics). Governments and the education sector should continue to future-proof the national curriculum to ensure that students are sufficiently equipped with both skillsets.
- The successful deployment of IoT training and education will require collaboration between industry, government and education sectors to:
  - attract and retain trainers and teachers with the appropriate skills and knowledge
  - enable access to or maintenance of IoT servers or systems with diverse data and sensors for student learning
  - establish cloud and network infrastructure to protect data, manage devices and perform data analytics.
- To support the development of IoT capabilities in RRR areas, VET providers, universities, external agencies and community networks could consider the expansion or adoption of regional study hub models, which provide infrastructure and academic support for students studying via distance learning at partner universities.
- Governments could consider supporting SMEs in their collaborations with industry and education providers so that employees are well-equipped to adapt to and adopt IoT technologies.

9

Research priorities will continue to evolve as IoT technologies mature. Proactive assessment of research gaps and consideration of associated funding towards these will ensure that the IoT is developed in a responsible and measured approach.

- Possible areas for research include:
  - New and novel IoT devices and applications to support a domestic IoT industry and encourage innovation.
  - The number and nature of IoT devices in Australia, as current research on these figures is nascent and still based on industry estimates.
  - Economic assessment of the value of IoT data produced under different property rights regimes and regulatory regimes.
  - The social and cultural dimensions of IoT use and impacts across the broad range of applications need to be better understood, particularly related to applications in homes, Indigenous and RRR communities. This could also include assessment of the potential uneven impacts of the IoT across vulnerable populations.
  - The use and acceptability of CAVs in the Australian context, including understanding the potential impact of legacy issues and backward compatibility, as well as the utility of CAVs to improve road safety by supporting existing road safety and emergency management systems.
  - Ongoing evaluation of the risks and potential impacts of increasing our dependence on connectivity for the provision of essential services, particularly in the context of disaster management for extreme climate events.
  - Environmental impacts of IoT manufacture and usage, including vendor lock-in, planned obsolescence and virtual wear-out.
  - Health impacts of radiofrequency electromagnetic energy (RF EME), including research in the millimetre wave spectrum and usage by emerging technologies, is needed to provide assurance to the Australian public.


HORIZON
SCANNING
ACOLA
AUSTRALIAN COUNCIL OF LEARNED ACADEMIES