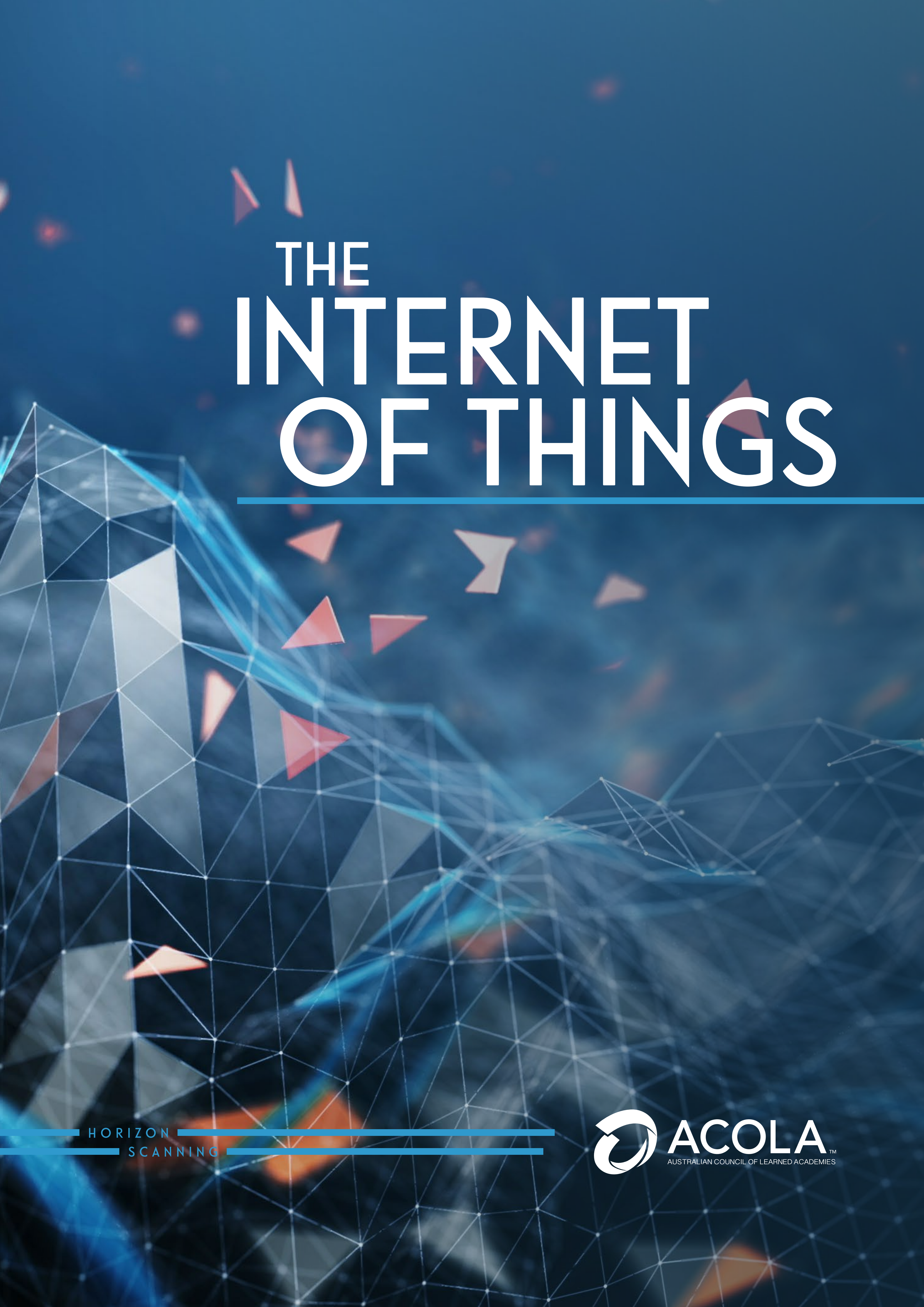


THE INTERNET OF THINGS

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

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

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.

THE INTERNET OF THINGS

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 report.

PROJECT MANAGEMENT

Stephanie Chan
Dr Lauren Palmer
Ryan Winn

HORIZON SCANNING

ACOLA™
AUSTRALIAN COUNCIL OF LEARNED ACADEMIES

ACOLA™
AUSTRALIAN COUNCIL OF LEARNED ACADEMIES

Working Together

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

ACADEMY OF THE SOCIAL SCIENCES IN AUSTRALIA

The Academy of the Social Sciences in Australia (ASSA) promotes excellence in the social sciences and in their contribution to public policy.

The social sciences are a group of like-minded academic disciplines that work on systematic development of logic and evidence to understand human behaviour in its social setting, including the nature of economic, political, and community activity and institutions.

ASSA is an independent, interdisciplinary body of over 650 Fellows, elected by their peers for their distinguished achievements and exceptional contributions across 18 disciplines.

ASSA coordinates the promotion of research, teaching and advice in the social sciences, promotes national and international scholarly cooperation across disciplines and sectors, comments on national needs and priorities in the social sciences and provides advice to government on issues of national importance.

Established in 1971, replacing its parent body the Social Science Research Council of Australia, founded in 1942, ASSA is an autonomous, non-governmental organisation, devoted to the advancement of knowledge and research in the various social sciences.

www.assa.edu.au

ATSE Australian Academy of Technology & Engineering

The Australian Academy of Technology and Engineering is an independent thinktank that helps Australians understand and use technology to solve complex problems.

We bring together Australia's leading experts in technology, engineering and science to provide impartial, practical and evidence-based advice on how to achieve sustainable solutions and advance prosperity.

We champion STEM excellence and contribute robust and practical thinking to Australia's big debates. Like you, we're curious about the world and want to create a better future.

We are a Learned Academy made up of almost 900 Fellows elected by their peers.

www.atse.org.au

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

Australian Academy of Science

The Australian Academy of Science (AAS) is a private organisation established by Royal Charter in 1954. It comprises more than 500 of Australia's leading scientists, elected for outstanding contributions to the life sciences and physical sciences. The Academy recognises and fosters science excellence through awards to established and early career researchers, provides evidence-based advice to assist public policy development, organises scientific conferences, and publishes scientific books and journals. The Academy represents Australian science internationally, through its National Committees for Science, and fosters international scientific relations through exchanges, events and meetings. The Academy promotes public awareness of science and its school education programs support and inspire primary and secondary teachers to bring inquiry-based science into classrooms around Australia.

www.science.org.au

Australian Academy of the Humanities

The Australian Academy of the Humanities (AAH) is the national body for the humanities in Australia, championing the contribution that humanities, arts and culture make to national life. It provides independent and authoritative advice, including to government, to ensure ethical, historical and cultural perspectives inform discussions regarding Australia's future challenges and opportunities. It promotes and recognises excellence in the disciplines that provide the nation's expertise in culture, history, languages, linguistics, philosophy and ethics, archaeology and heritage. The Academy plays a unique role in promoting international engagement and research collaboration, and investing in the next generation of humanities researchers.

www.humanities.org.au

ASSOCIATE MEMBER

Australian
Academy *of* Health and
Medical Sciences

The Australian Academy of Health and Medical Sciences is the impartial, authoritative, cross-sector voice of health and medical science in Australia. We are an independent, interdisciplinary body of Fellows – elected by their peers for their outstanding achievements and exceptional contributions to health and medical science in Australia. Collectively, they are a representative and independent voice, through which we engage with the community, industry and governments.

The Academy is uniquely positioned to convene cross-sector stakeholders from across Australia to address the most pressing health challenges facing society. We focus on the development of future generations of health and medical researchers, on providing independent advice to government and others on issues relating to evidence based medical practice and medical researchers, and on providing a forum for discussion on progress in medical research with an emphasis on translation of research into practice.

www.aahms.org

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

CONTENTS

FIGURES

TABLES

BOXES

SCENARIOS

CASE STUDIES

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.

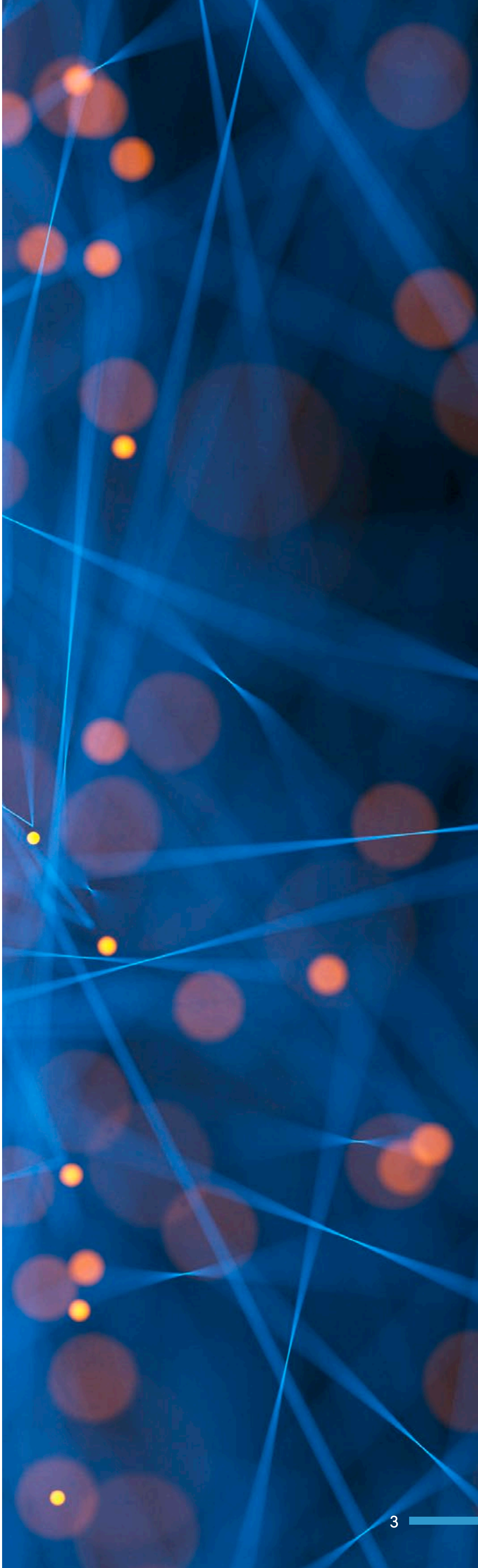
Sustainability is another key issue that will require consideration over the next decade. While IoT devices and systems offer benefits, the energy to power these systems is likely to require one to five percent of the world's electricity by 2050. As our report demonstrates, there may even be rebound 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.

BL Fox.

Professor Bronwyn Fox FTSE



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.

METHODOLOGY

ACOLA Horizon Scanning Reports are primarily developed by leading academic experts across Australia and internationally. As the IoT is an emerging field and interdisciplinary academic research in some areas in this field is still nascent, the report has also drawn on evidence, data and reports from industry and consultant groups. ACOLA acknowledges that these sources may be based on interest groups' own values, goals and outcomes. However, as this report is a horizon scan over the next decade, these sources provide valuable context to the currently available knowledge and research across the sector as a whole. These views were validated with other sources where possible.

In 2019, ACOLA also underwent extensive consultation with stakeholders from government, industry and community to seek expert opinions on attitudes, efforts and investment in the current Australian IoT sector. Key discussion questions were developed by ACOLA and the Expert Working Group to direct and inform these consultations. Over 40 targeted stakeholders were approached based on recommendations by the Expert Working Group and government project sponsors. From September to December 2019, ACOLA conducted 24 one-hour consultations with four Australian Government agencies, six state and local governments, two community groups, seven industry experts and five academics from research organisations. ACOLA and the Chair of the Expert Working Group also consulted with four key government agencies in Canberra in September 2019. Following these consultations, ACOLA assessed the responses and drew out critical areas or themes; these have been used to develop this report and its key findings. A list of the stakeholders consulted can be found in the Evidence Gathering section of this report. Information from these sources has been included in the report alongside current academic research.

The report underwent academic peer review, and eight Australian Government agencies and an industry expert also reviewed the report.

Due to the rapid growth and complexity of this field, there are inherent uncertainties in the available research, literature and stakeholder consultation responses. This report is based on the best and most robust information available at the time of the study.

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.

INTRODUCTION

The IoT will provide opportunities to improve the way Australians live, and increase productivity and efficiency in a variety of sectors. There is much discussion about the IoT across government and industry, particularly in relation to 'smart cities', but the technology is not well understood by the public or Australian institutions and agencies.

This report aims to provide a greater understanding of the IoT and explore the ways it can benefit Australia if managed appropriately. Management of the IoT is important; as with any emerging technology, it can pose potential risks, harms or unintended consequences. These need to be identified and addressed, so that the benefits of the IoT can be realised without intensifying social and economic problems, causing privacy and security issues or creating socioeconomic disadvantage.

Potential of the IoT in Australia

There are already more IoT devices on Earth than humans and this number will only increase (Hung, 2017). The economic and technical incentives built into the technology have led to IoT devices becoming increasingly ubiquitous throughout society. More data mean greater insights, leading (at least in theory) to improved efficiency, more desirable products and services, and better economic returns (Manyika et al., 2015). As a result, the IoT presents Australia with many new opportunities for economic growth and prosperity.

In Australia, innovation in the IoT is well underway. Governments and local councils have already begun to capture the value of the IoT to enhance the liveability and sustainability of their communities. With the ability to optimise homes, cities and regions, the IoT can improve living standards for Australians. However, Australia can be much more proactive about harnessing the potential economic benefits of the IoT to remain globally competitive. A strong domestic IoT industry will have flow-on effects for the employment sector and can support the development of skills and the creation of new jobs, in particular for data scientists, software and systems engineers, full stack developers, cybersecurity professionals, and communications and network designers.

While the IoT offers great potential for Australia, it does come with challenges and risks. Issues of data collection and management, privacy and security will be important considerations moving forward. The potential for changes in employment conditions for Australians, such as re-skilling and up-skilling workers, even while new employment opportunities emerge, requires careful consideration. IoT technologies may also lead to unintended consequences such as the exacerbation of existing inequalities for socially disadvantaged groups or family violence.

The structure of the report

As with all ACOLA Horizon Scanning reports, this report uses an interdisciplinary approach to assess the opportunities, impacts and risks of the IoT in Australia over the coming decade. While large international technology firms will drive aspects of the IoT, this report describes areas where Australian stakeholders can focus their efforts to lead the development and implementation of the IoT in our cities and regions.

Chapter 1 provides an overview of IoT developments globally and in Australia.

Chapter 2 assesses the applications of IoT in smart cities and regions.

Chapter 3 assesses security and privacy issues.

Chapter 4 assesses enablers for deployment and sustainability considerations.

Chapter 5 assesses social and community considerations.

Chapter 6 assesses jobs, skills, education and research.

Key considerations at the beginning of each chapter provide a summary of the main points, and are categorised by their short, medium and long-term impacts, informed by our Expert Working Group.

The following areas will have a significant impact on legislative, judicial and corporate areas and are discussed in the Appendices:

- international context: the development and implementation of the IoT internationally will influence the governance of the IoT in Australia, so background information on the international context is provided (Appendix A)
- technological infrastructure: the IoT will increase pressure on data-transmission networks and data storage centres (Appendix B)
- security vulnerabilities: attacks in IoT typically occur in five areas which require mitigation strategies to minimise the risk of harm (Appendix C)
- Australia's privacy framework and its applicability to IoT: assessment of the *Privacy Act 1988 (Cth)* will require review in a number of areas to ensure there is adequate protection for consumers as novel applications of IoT increase (Appendix D)
- accountability and liability: overlapping contracts from multiple service providers and device operators will complicate the process of assigning blame and resolving problems when IoT systems generate harms (Appendix D).

Other social considerations of the IoT are described in Appendix E. National use cases are interspersed through the report, with international use cases across different industries outlined in Appendix F.

The report does not examine in detail some of the technical aspects of IoT technology, such as AI and machine learning, as these are covered in the ACOLA report on artificial intelligence, *The effective and ethical development of artificial intelligence: an opportunity to improve our wellbeing* (Walsh et al., 2019). Data considerations and privacy implications, relevant to IoT and other emerging digital technologies, are also discussed in more detail in the ACOLA artificial intelligence report.

CHAPTER 1
THE INTERNET OF THINGS LANDSCAPE

Chapter overview

- Estimates of the economic value of the IoT differ widely, as definitions and key indicators for measurement vary. However, in 2018, the International Data Corporation forecast that IoT spending could grow at an annual compound rate of 13.6 percent from 2017 to 2022 to reach US$1.2 trillion in 2022.
- 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. PwC has estimated that on average, a two percent productivity increase per annum could be realised across each of these five industries in Australia representing 25 percent of Australia's GDP in 2018: construction, healthcare, mining, agriculture, fishing and forestry, and manufacturing.
- It is estimated that there will be 29 billion connected devices in the world by 2022, of which around 18 billion will be related to the IoT.
- In 2018–19, there were 16 million IoT-connected devices installed in Australia, and it was forecast that more than 47 million smart devices will be installed in Australian homes by 2022.
- Large investments and international efforts by both industry and governments demonstrate a shared sense of urgency to capture the anticipated economic value from IoT applications.
- Interoperability remains a critical issue for devices, networks and platforms, which can cause multiple problems in IoT networks, including vendor lock-in, difficulty in plugging IoT devices into non-compatible platforms and a lack of cross-platform and cross-domain IoT applications.
- Across industry, governments and international bodies, standards are currently heterogenous, with competing standards and initiatives being developed across different aspects, including security, privacy, architecture and interoperability. However, there is a growing recognition of the need for international collaboration through the use of international forums and standards making bodies.

- The lack of data sharing incentives, tools and associated security concerns means that access by government to data collected by companies is currently limited. However, national and state and territory governments are beginning to make use of open data platforms and data sharing initiatives to encourage greater transparency, accountability and innovation.
- Businesses are collecting and analysing data from IoT devices in increasingly sophisticated ways with AI and machine learning techniques to maximise value to both users and company revenue streams.
- Connectivity is an important enabler of IoT; however, people living in RRR areas, even in some areas very close to major cities, sometimes lack reliable internet access.

1.1 Definition of the Internet of Things

It is difficult to provide a concise definition of the IoT due to the complexity, breadth and inconsistency of what has been implied by the term over time, in both its technical and social dimensions (Manwaring and Clarke, 2015). Scholarly work has tended, although not exclusively, towards a narrower definition, concentrating on the relevant enabling infrastructure. However, the popular explanation of the IoT tends to be broader in its scope and includes 'smart' devices, as well as incorporating (usually only by implication) related technologies such as ubiquitous and pervasive computing, ambient intelligence and smart environments.

For the purposes of this report, the authors prefer the Organisation for Economic Co-operation and Development (OECD) definition:

> IoT refers to an ecosystem in which applications and services are driven by data collected from devices that sense and interface with the physical world. In the Internet of Things, devices and objects have communication connectivity, either a direct connection to the internet or mediated through local or wide area networks. (Organisation for Economic Co-operation and Development, 2016).

Typically, an IoT device consists of an embedded sensor and/or an actuator (hardware), a microprocessor with software, as well as communication infrastructure. These components enable data collection, handling and communication. A typical IoT device senses data and sends it to a separate location for processing via the internet or private network; it also receives data and performs limited actions. IoT devices can be small, are often resource constrained and are typically embedded in other real-world objects. Please refer to Appendix B for further information.

Many IoT devices are also components of 'product–service packages', where services are provided alongside the IoT device as essential or optional elements of the functionality provided. Many IoT devices may be nested within a larger IoT device or form elements of a larger distributed system. Issues arising out of IoT devices may relate to a single IoT device, to the whole or to some elements of the 'ecosystem'[3] in which the IoT device participates. Today, the IoT encompasses billions of connected devices, many of which are integrated with industrial services and infrastructure, such as energy services, water, transport and logistics, consumer services or retail.

Some definitions of IoT devices exclude smartphones and tablets because they are used for general computing processing. However, when considering the social impact of the IoT, the context-specific role of these devices, particularly smartphones, cannot be ignored. These devices and the applications installed on them form an integral part of many systems involving other IoT devices, either as a remote controller or as the primary device to which data are communicated to people in an intelligible form.

Box 1: Definitions: sensor, actuator and microprocessor

Sensor: records and transmits data via the internet or through private networks about the physical environment, including movement, sound, light, electrical potential, temperature, moisture, location, air quality and body metrics (such as heart rate and variability, skin conductivity and blood flow volume) (Swan, 2012).

Actuator: component that uses collected and processed data to effect a change in the environment such as temperature control (Sethi and Sarangi, 2017).

Microprocessor: component that accepts data recorded from sensors (input) and processes it to execute a wide variety of applications (output); must be able to dynamically adapt to various execution scenarios and data characteristics (Adegbija et al., 2018).

[3] The term 'ecosystem' was adopted from Noto La Diega and Walden (2016) and Millard et al. (2017).

Scenario 1: The connected home

It is 5:30 am and the sky is just beginning to brighten over Perth, WA. The Singh family are still sleeping but their connected home IoT platform has been busy. It has been monitoring the four family members' sleeping patterns and, based on data collected on their daily sleep cycles, is deciding on the best time to wake them. Combined with data on weather and traffic conditions accessed from local news agencies, it decides that the optimal time to wake up Priya Singh is at 6:30 am. This will allow her to comfortably go through her morning routine and get to work by 8:30 am. The home IoT platform directs her smart bracelet to vibrate briefly at intervals of 10 seconds, waking her with minimal disturbance. Her partner Jai is still asleep and prefers to wake up with natural light. Noting this, the home IoT platform sends a notification for the blinds to open in their room at 7 am.

As Priya steps into the bathroom, the movement sensors turn on the bathroom lights. The home IoT platform has already turned on the home's energy systems, which were on 'energy-saving' mode as the family slept, with power only for essential functions such as the fridge and for emergencies. While Priya gets ready, the home IoT platform analyses daily rates for electricity and decides that it will run the washing machine and dishwasher at 11:45 am, to make use of the best available off-peak electricity rates. The home IoT platform notes that the house solar panels have accrued excess solar power and directs it to be auctioned off through the city's decentralised grid system.

The promise of IoT technologies lies in the data that is generated by these connected devices that will have the ability to create 'big data' ecosystems (Organisation for Economic Co-operation and Development, 2016). This data can be used to analyse patterns, anticipate changes or alter an object or the environment to achieve the desired outcome. This will drive innovation and research, as well as optimisation of the services and products that generated this data. For example, a smart mobility scenario could include sensing and analysis of traffic flow, which enables control responses to adjust traffic lights to manage congestion.

Advancements in machine learning and AI have enabled the development of algorithms and neural networks to analyse and process data, sometimes within the device or through edge computing. This means that decision making may no longer require human interaction or direct communication (Walsh et al., 2019), further enhancing our ability to aggregate and analyse data in an agile, on-demand way and with reduced management effort (Organisation for Economic Co-operation and Development, 2016).

Figure 1 outlines some of the settings where IoT devices may be used to optimise processes and systems.

Figure 2 provides an overview of the horizontal architecture of an IoT ecosystem. As discussed, devices typically include sensors and/or actuators, as well as software and communications components for device management. Collected data are then sent through a network to a remote location such as a middleware software platform (e.g. a centrally located cloud service). This middleware layer acts as the intermediary between devices, sensors, operating standards and applications and also provides privacy and security functions for the system (Bandyopadhyay et al., 2011). It manages and stores the large volumes of collected data, analysing and processing it for a range of applications including visualisations and alerts. For example, in water management, data collected from sensors in a network of pipes would be analysed and processed in the middleware layer, and an alert would be sent to the maintenance team if a leak were detected. Early leak detection means that the pipe could be quickly repaired, minimising disruption to consumers and reducing cost and repair efforts for the water management company.

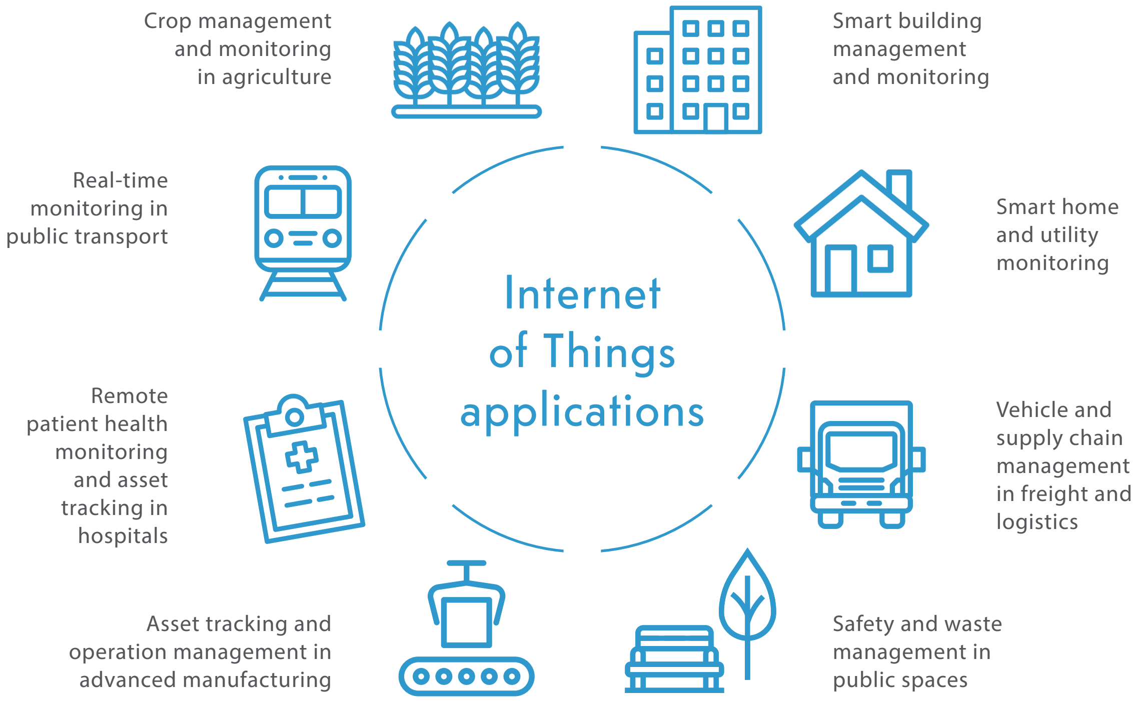
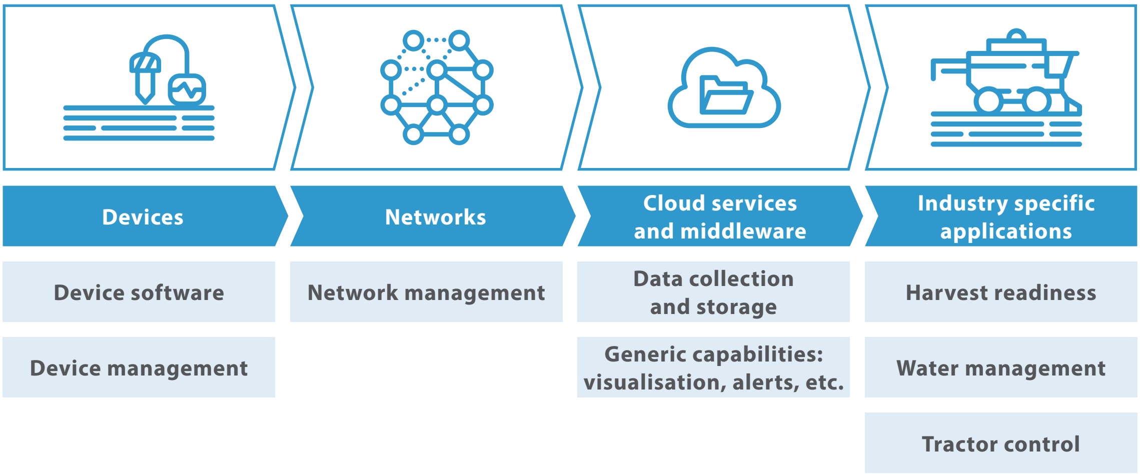

Crop management and monitoring in agriculture
Smart building management and monitoring
Real-time monitoring in public transport
Smart home and utility monitoring
Internet of Things applications
Remote patient health monitoring and asset tracking in hospitals
Vehicle and supply chain management in freight and logistics
Asset tracking and operation management in advanced manufacturing
Safety and waste management in public spaces

Figure 1: IoT applications



Devices	Networks	Cloud services and middleware	Industry specific applications
Device software	Network management	Data collection and storage	Harvest readiness
Device management		Generic capabilities: visualisation, alerts, etc.	Water management
			Tractor control

Figure 2: IoT architecture components

Adapted from Bradlow, 2019.

1.2 IoT applications

IoT devices are increasingly appearing in all parts of society, business and industry, public spaces and in our personal spaces and homes. While the application of the IoT can vary across different settings depending on the uses and capabilities that are required, the data captured has great potential to optimise existing processes and products. Given the low cost of sensors and increasingly ubiquitous network connectivity, devices are able to operate at a continental scale. Example applications are listed below:

- *Locational awareness* will enable the sensing of people and objects for use in mobile asset and commodity tracking, fleet management, traffic optimisation and safety.
- *Environmental awareness* will be based on sensors collecting a range of data to monitor the environment: for example, temperature, humidity, noise, visibility, light intensity, radiation and pollution (CO, CO_2, etc.).
- *Medical monitoring* will allow health data to be remotely collected from devices worn by patients, providing medical practitioners and users with information to optimise advice and alerts, enhancing personalised, self-managed healthcare.
- *Industrial monitoring* will involve incorporating sensors into machinery, vehicles or other assets in the field to understand the health and efficiency of equipment and enable accurate and proactive maintenance.
- *Real-time remote operation* of assets in industrial contexts such as factories or construction, healthcare and educational settings and in smart homes will increase optimisation of products and services, and provide greater access, comfort and convenience.

Table 1 provides a comparison of example IoT applications in an industrial, consumer and public-space context to demonstrate the various benefits and uses that can occur across a range of different settings.

1.3 Data considerations

As more IoT devices appear in businesses, industries, public spaces and in our homes, it will be important to raise public awareness of the data considerations associated with these devices so that consumers can assess the risks and benefits in an informed manner.

A key challenge for awareness is that IoT devices often take the form of seemingly innocuous everyday objects (e.g. smart televisions, front door locks and kettles). These devices have the ability to unobtrusively collect and share data without our knowledge or action. While this ability makes IoT devices useful and convenient, this also poses concerns. For example, smart home devices produced by companies such as Google, Amazon and Microsoft allow consumers to conveniently automate processes in their homes, using data from their home environment (hyper-local data). These companies analyse the data with AI and other techniques in increasingly sophisticated ways, using it to maximise value not only to users but also for their own purposes to increase revenue streams, for example by using customer insights to improve product development.

Table 1: Comparison of IoT applications

Context of IoT			
	Industrial	**Public space/Government**	**Consumer**
Application	Monitoring critical infrastructure in energy, manufacturing, mining, health, logistics, transport.	Transport (e.g. connected cars, congestion management), smart energy (e.g. lighting), waste management.	Smart home management, home energy management, some wearables and fitness trackers,[4] smart locks, healthcare, ageing in place.
Benefit	Productivity and efficiency.	Efficiency of public services and consumer benefits, including consumer-focused services.	Quality of life, convenience, energy savings, health improvements, time efficiency.
IoT device sensor capabilities	A connected network of sensors on assets provides real-time data to monitor inputs and outputs.	Sensors embedded into existing infrastructure, including street lighting, utilities or in transport vehicles such as trains or trams.	Sensors embedded in small, accessible devices or wearables.
Use case example	National transport company SCT Logistics has deployed sensors to track and monitor its rail, freight and road transport fleet to better understand usage and utilisation rates (Prime Mover, 2019).	In Newcastle, NSW, a network of sensors deployed on smart poles will measure environmental conditions such as air quality, water usage and humidity to improve sustainability and liveability. Sensors on smart bins and in parking areas, will monitor the performance of urban systems and assets.	Smart home devices improve efficiency and provide convenience in the home, while wearables monitor heart rate, sleeping patterns, activity and body weight to improve quality of life and health.

[4] This excludes wearable and fitness trackers that are sensor extensions of a smartphone app rather than IoT devices in their own right.

Government agencies, in contrast, must abide by more stringent privacy obligations than companies regarding the use of citizen data. Governments currently have limited access to the data collected by companies from the use of smart home devices due to security concerns and a lack of data sharing incentives and tools. However, they are beginning to make use of open data platforms and data sharing, providing public access to transport and health datasets to facilitate greater transparency, accountability and to encourage start-ups to use this data in innovative ways (see Case study 19, Chapter 2).[5]

IoT applications in industries such as manufacturing, logistics, transport and utilities require far more stringent data security and reliability requirements for the control and operation of systems compared to consumer-orientated applications.

While dta are being gathered from an increasing number of sources and at lower cost than ever before, questions and challenges remain about how homeowners, industries, cities, regions and governments understand and manage data collection, including:

- ownership of data
- making collected data visible and accessible
- determining and guaranteeing levels of data accuracy and authenticity
- protecting citizen, commercial and state rights
- ensuring data are accurate
- protecting against intrusion and disruption
- ensuring that socioeconomic disadvantage is not perpetuated or exacerbated by inaccurate or punitive use of personal data.

1.4 Economic review

1.4.1 International estimates

Economic analysis of the value of the IoT has been limited in both international and domestic contexts. As is the case generally for the analysis of technologies, economic attribution as a direct result of IoT can be difficult to quantify. This is because technologies act as enablers within and across industries, and are used in conjunction with other technologies — in the case of IoT, this includes AI and edge computing. As such, caution should be taken when attributing the direct impact of IoT on economic growth and productivity.

Most reports assessing the global economic impact of the IoT analyse productivity-enhancing effects across a range of key industries (through the lowering of costs), with revenue-enhancing improvements in services as a second order effect. The economic impact is quantified by estimates of business *spending* on IoT adoption, and further supported by the growth of IoT devices (i.e. capital).

In 2015, McKinsey forecast that the potential global economic impact of the IoT could reach US$11.1 trillion per year by 2025 (Manyika et al., 2015). The McKinsey report, which used a bottom-up, settings-based estimation methodology, emphasises that much value capture from IoT comes from integrating systems and allowing data in one setting to be reused in others, and from more and better information-facilitated, automated decision-making.

[5] See open data platforms such as Data.NSW and the Open Data Portal for Western Australia.

As the industry matures, global estimates have become more moderate. A Bain & Company survey of more than 600 executives found that, while businesses recognised the value of the IoT, many had tempered their expectations about the speed of IoT adoption, acknowledging that applications would take longer to implement and generate profits (Bain & Company, 2018). In 2018, the International Data Corporation forecast that IoT spending could grow at an annual compound rate of 13.6 percent from 2017 to 2022 to reach US$1.2 trillion in 2022, with the consumer sector, insurance and health providers being the three leading sectors by spend (IDC, 2019). The International Data Corporation also indicated that discrete manufacturing and transport could be the largest industries for IoT expenditure, with each industry anticipated to exceed $150 billion by 2022 (IDC, 2019).

1.4.2 Global estimate of number of devices

Countries have only recently begun collecting data on the number of IoT devices. This has been challenging given the complexity in defining the IoT and finding a consistent metric to capture the number, nature and type of IoT devices and connections (Organisation for Economic Co-operation and Development, 2018a). In 2019, ACMA quoted industry estimates of 29 billion connected devices in the world by 2022, of which around 18 billion will be related to the IoT (Australian Communications and Media Authority, 2019a). Alternative estimates based on industry data from telecommunications carriers also provide some utility. Ericsson provided more conservative figures, estimating that there were 1.5 billion IoT cellular connections in 2019 and expecting this figure to reach 5 billion by 2025 (Ericsson, 2019).

1.5 Global developments

Large investments and international efforts by both industry and governments demonstrate a shared sense of urgency to capture maximum economic value from IoT applications. There are many lessons that can be learnt from countries that have been successful in the implementation of IoT systems and networks, such as the European Union (EU), Germany, United Kingdom (UK) and South Korea. An overview of key developments by countries that have shown leadership or innovation in IoT are outlined in Appendix A, with examples of international use cases in Appendix F.

1.5.1 Standards

As a response to its inherent complexity and applicability across sectors, a multitude of competing standards, regulations and initiatives have been developed for the IoT around the world, including standards for security, privacy, architecture and interoperability. However, this heterogeneity is difficult to navigate, and there is a growing recognition of the need for collaboration through international forums and standards-making bodies. IoT consortiums established by industry leaders and governments are also beginning to work collaboratively to define sets of requirements rather than standards.[6]

[6] For example, in 2016, the Industrial Internet Consortium and I4.0 began to collaboratively map their reference architectures and identify opportunities for collaboration. The Industrie 4.0 and Japanese Robot Revolution and Industrial IoT Initiative have an enhancement of collaboration agreement, and an agreement of advancement between the Japanese Ministry of Economy, Trade and Industry and German Federal Ministry for Economic Affairs and Energy (see Japanese Ministry of Economy, Trade and Industry, 2016).

Key developments include:

- The International Organization for Standardization (ISO), which Australia is a member to, has developed a number of IoT-specific standards for architecture, with further standards in development.[7]
- The European Standards Organisation launched the European Telecommunications Standards Institute (ETSI) Technical Specification 103 645, the first globally applicable industry standard on cyber security for internet-connected consumer devices in 2019. This is currently being transposed into a European Standard as April 2020.
- The General Data Protection Regulation provides EU citizens with the right to 'opt out' of data sharing and the flexibility to withdraw consent, even if previously given.
- The Internet of Things Cybersecurity Improvement Act of 2019 is currently being considered by the United States (US) Senate. This Act would require US government agencies to apply mandatory security regulations in the use of IoT devices. Industry initiatives in the US include the National Institute of Standards and Framework's Cybersecurity Framework, the Cybersecurity Maturing Model Certification and the Health Insurances Portability and Accountability Act.
- The UK is considering legislation that would require IoT devices to be sold with labels indicating the security measures or vulnerabilities of that device.
- International 5G standards are currently in development through the 3rd Generation Partnership Project.[8]
- The International Telecommunication Union (ITU) World Radiocommunications Conference was held in October-November 2019, with agreements on the global use of radio-frequency spectrum and satellite orbits signed by 3,400 delegates from 165 member states.

1.5.2 Privacy and security considerations

Internationally, there is a growing awareness and action being taken to address the privacy and security challenges that the IoT raises. These include the development of non-binding codes of practice for IoT consumer goods and connected and autonomous vehicles (UK), the implementation of the EU Cybersecurity Act 2019 (EU) and adoption of the GDPR and the NIS Directive: The directive on security of network and information systems (EU and UK) (Brass et al., 2019). In 2019, the Five Eyes nations (Australia, Canada, New Zealand, UK and US) jointly signed a statement of intent recognising the cybersecurity challenges that would arise from the IoT and to promote ongoing international alignment on IoT security. There is also an increasing number of guidelines and standards being driven by industry consortiums and associations.[9]

[7] These include ISO/IEC 30141 for standard reference-architecture, ISO/IEC 27001 for best-practice information security management systems, ISO/IEC 27032 for cybersecurity, ISO/IEC 27035 for incident management, ISO/IEC 27031 for ICT readiness for business continuity and ISO/IEC 22301 for business continuity management systems focusing on recovery and access and security after an incident.

[8] The 3rd Generation Partnership Project is a consortium of standards organisations that develop protocols for mobile communications. National and regional organisation partners from Japan, the US, China, Europe, India and South Korea also collaborate with a number of market representation partners to develop standards such as GSM and related 2G and 2.5G standards, and LTE and related 4G standards.

[9] See work by the IoT Security Foundation, Global Systems for Mobile Communications Association or Open Web Application Security Project (Brass et al., 2019).

For example, the World Economic Forum has proposed agile governance for emerging digital technologies as a key driver of the Fourth Industrial Revolution (Brass et al., 2019). However, these guidelines and best practices remain non-binding and require buy-in from industry (Brass et al., 2019).

Overall, the landscape is heterogenous and complex, with the IoT 'blurring the boundaries between established standards and regimes for physical security, cybersecurity, safety, liability for defective products, data protection and trust/trust worthiness' (Brass et al., 2019a, p. 3). Research has shown that the IoT is often not considered at global cybersecurity policy forums, partly due to the failure in bringing experts and policy-makers together and partly due to the difficulties in addressing rapidly changing security problems through conventional governance mechanisms (Brass et al., 2019).

1.5.3 Social and cultural considerations

The social and cultural aspects of the IoT are complex, as issues of trust, social norms and expectations, social imaginaries, surveillance, control, privacy and the political dimensions of personal data use and misuse overlap with work on standards and cybersecurity.

Research by IoTUK, a national program to facilitate the adoption and development of the IoT in the UK, has considered how consumers can take precautions to mitigate risks from cyberattacks in an IoT environment (Blythe and Lefevre, 2018). The study found that security advice needed to more comprehensively consider user goals, motivations and capabilities, otherwise users would prioritise convenience of use over security. A holistic approach was required to encourage behaviour change on many levels – not only by users but also by manufacturers and retailers. Another project considered the relationship between the IoT, gender and young people, investigating the likely privacy and security challenges arising for family violence survivors or children using IoT devices (Brass et al., 2019). The increased adoption of IoT in private environments such as homes raises further issues regarding personal information and the right to privacy.

Recommendations from this research have indicated that there is a need to expand the definition of technology-facilitated abuse and other criminal acts to include the IoT. In addition, statutory and non-government services need to be educated about the risks that the IoT can pose to vulnerable groups, including children and socioeconomically marginalised and disadvantaged people (Brass et al., 2019). There are potential harms that go well beyond privacy risks and threats to personal safety, health and wellbeing, such as racism, social exclusion, loss of access to social services and support, and exposure to stalking and assault.

More generally, there is a recognition that many people have an 'education gap' about the IoT and need to be supported to gain better understanding of the IoT and its applications (Brass et al., 2019).[10] In response to some of these concerns, a Privacy, Ethical and Social Impact Assessment has been developed by the European Commission's Community Research and Development Information Service to help designers

[10] The research highlighted that improved education of the public may not be enough. Regulation is needed to protect the public against those who want to exploit their personal data; or in contexts in which they are forced to use IoT technologies, for example, to receive social security payments or in educational settings; or when abusive partners have secretly installed surveillance systems.

and innovators proactively self-assess the safety and ethical considerations in the development phase of IoT technologies (European Commission, 2017).

As of August 2020, the global outbreak of COVID-19 has allowed for new levels of surveillance by governments in some countries. Real-time location data and emerging technologies such as facial recognition, contact tracking apps and drone surveillance are being deployed by some governments for rapid contact tracing and monitoring actual and suspected infections. This raises questions about deploying these types of powers for epidemiological necessity and proportionality (Funk, 2020). It will be important to consider the future implications of IoT applications that enable these types of surveillance programs to ensure that they align with human rights principles and citizen expectations of privacy and security.

1.6 Australian context

1.6.1 Australian economic estimates

As noted in the discussion on international estimates (section 1.4.1), IoT economic analysis has been limited. In Australia, recent research by the Bureau of Communications and the Arts Research (BCAR), and by PricewaterhouseCoopers (PwC), provides some insight into the national impact of IoT to date and potential future growth. The BCAR research estimates IoT activity as a measure of its contribution to the Australian economy (measured on a satellite accounts basis) as of 2016–17 (Bureau of Communications and Arts Research, 2020), while the PwC report assesses IoT's potential in generating future productivity improvements to Australia's economy.

1.6.1.1 Contribution of IoT activity to Australia's economy

The BCAR's research utilised Australia's national accounts to estimate the contribution of IoT activity to Australia's economy for five years, from 2012–13 to 2016-17. It estimates IoT activity[11] alongside two broader measures of digitalised activity in Australia's economy – ICT and digital activity. The estimates showed that IoT activity's contribution to the economy has steadily grown in recent years, and is unlikely to abate as opportunities and industry applications become clearer. This has the potential to create exponential economic growth, which is further demonstrated by PwC's analysis.

BCAR's analysis showed that growth in gross value added (GVA)[12] of IoT activity has outpaced the Australian economy overall since 2014–15. This is consistent with the impact of technological advances on creating digitally-enabling goods and services, such as computer system design and telecommunications services. The main industry contributor to growth in IoT activity was the information media and telecommunications (IMT) industry. Growth was even greater once price effects are removed, as prices over this period fell due to cheaper and more competitive telecommunications technology and network infrastructure.

[11] BCAR defines IoT activity as the final goods and services produced that enable an internet connection between physical objects, and it consists of hardware, software, telecommunications, internet of service providers (ISPS), support services and big data.

[12] GVA is a measure of the contribution to domestic production made by an individual producer, industry or sector, and measures output minus the value of goods and services used up in the process of production. It does not include net taxes (which GDP does) and therefore provides a more accurate measure of economic activity by industry.

In terms of current price measures,[13] BCAR's analysis showed 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 (Figure 3). As a share of GVA of the overall economy, this was an increase from 4.4 percent in 2012–13 to 4.5 percent in 2016–17 (Figure 4).

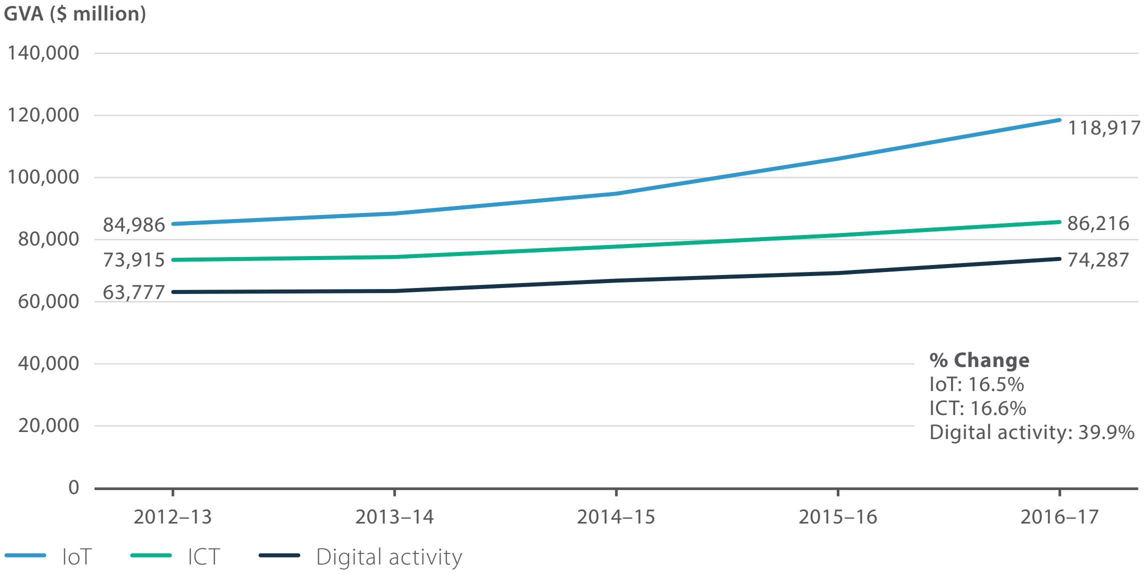


Figure 3: IoT, ICT and digital activity GVA measured by current price measures, 2012–13 to 2016–17

Source: ABS cat. 5215, 5217; BCAR calculations.

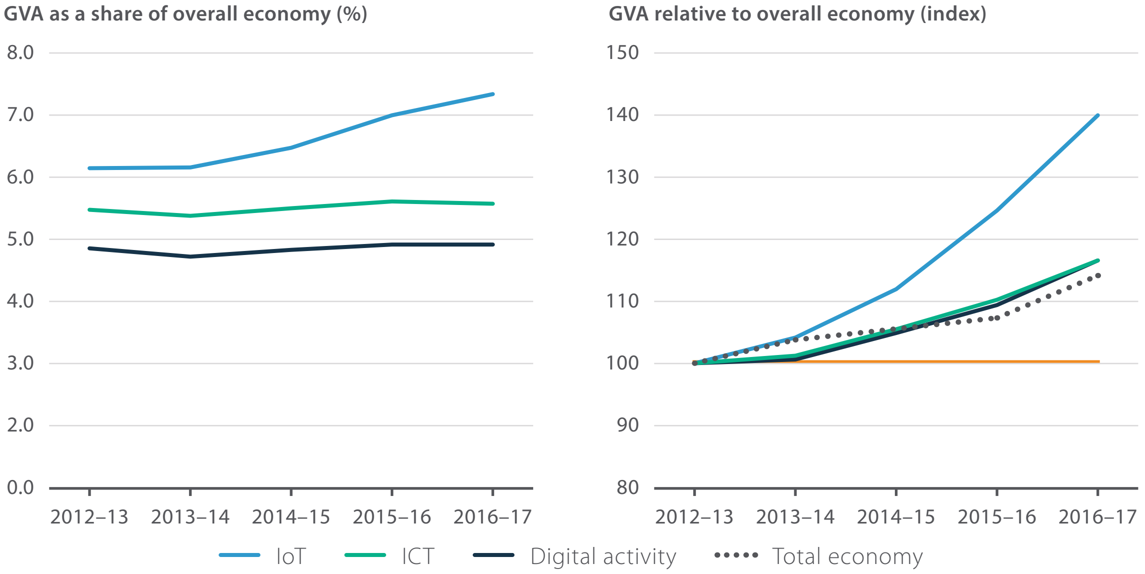


Figure 4: GVA as a share and relative to the overall economy by current price measures, 2012–13 to 2016–17

Source: ABS cat. 5215, 5217; BCAR calculations.

Note: The right panel of the figure shows an orange line at 100 that represents the base year index of 2012–13. The area above this line represents growth since 2012–13, while the area below represents contraction. The dotted line represents GVA growth for the total Australia economy relative to the base year.

[13] Current price measures the value of goods and services based on their prices at the time of transaction. This measure is not adjusted for inflation to demonstrate the influence of price changes over time.

1.6.1.2 Assessing future outlook of the IoT

PwC's analysis focused on the future outlook of the IoT, assessing potential IoT use cases and their impact on Australian industries.[14] Impact of the IoT varied significantly across sectors, but industries that were asset-heavy, device-rich and involved significant physical labour were likely to derive greater benefit. The highest impact was across five sectors that represented 25 percent of the GDP in 2016–17: construction, agriculture, fishing and forestry, healthcare, mining, and manufacturing (PricewaterhouseCoopers and Australian Computer Society, 2018).

PwC found that the IoT would enable a range of benefits across these industries, including: efficiency improvements; asset management; workplace safety; and environment management. It was estimated that on average, a two percent productivity increase per annum could be realised across each of these five industries. In addition, the competitiveness of Australia's exports is increasingly being challenged, primarily due to the higher relative costs of domestic production. While adopting IoT technologies could significantly improve our export competitiveness, security, organisational and structural challenges would constrain adoption rates.

As demonstrated by BCAR's research, we have already seen the significant impact of IoT on the Australian economy. The opportunity cost for not capturing the full benefits of IoT is considerable, and is likely to impact on our economic productivity and global competitiveness if not fully realised, especially as countries bolster their own IoT and digitalisation efforts. Ongoing innovation and competition in the ICT and telecommunications sector are also likely to make devices and network infrastructure cheaper and more accessible, which will likely increase the use of IoT across sectors over the next decade. Australia should continue to focus on areas of competitive advantage to maximise the economic gains from the IoT.

1.6.2 Additional economic effects

In addition to forecasting the economic value of the IoT, there is also strong benefit in examining the likely structural effects that may occur as a result of the data collected from an IoT-permeated economy.

1.6.2.1 Increased automated decision making

There will be a shift in the locus of decision making from humans to machines. The increased automation of decision making shows up in different ways in different sectors. This shift will have by far the greatest impact on the economy, changing the types of goods and services offered, the types of firms that exist, as well as the regulatory and taxation environments needed to support this type of economy.[15]

[14] To forecast the potential value of IoT on Australia's economy, PwC undertook broad secondary research into a set of generic use cases across Australian industries including services, education and training, healthcare, arts and recreational services, financial and professional services, as well as consulting with a range of industry experts to understand the IoT applications across sectors. The potential impacts of the IoT within an industry were then combined with the overall relevance of the sector to the economy based on 2016-17 GDP.

[15] The *ARC Centre of Excellence in Automated Decision Making and Society*, based at RMIT University, is an example of the sorts of research centres that are exploring the challenges this brings.

1.6.2.2 Data as an asset

There will be an increase in the quantity and value (or economic importance) of data, and therefore a corresponding increase in the value of data property rights. This contrasts with the industrial-era model of data as a quasi-public good that is regulated by government. This will drive the importance of data property rights (cf. data human rights, data regulation, General Data Protection Regulation, etc.) and the emergence of data markets. Further economic analysis should seek to estimate the value of data produced under different property rights regimes and under different regulatory environments. Distributional consequences of the growth of data assets should also be considered.

1.6.2.3 Centralised versus decentralised data models

The economic impact of the IoT can be envisaged through two different models with very different economic evolutionary consequences (Manyika et al., 2015). A centralised data model focuses more on the impacts of centralised oversight of the investment, production and allocation of goods, while a decentralised data model tends toward a freer market economy. IoT technology will develop along different pathways depending on whether data is centralised or distributed.

The IoT can facilitate a more centralised economic command and control model of an economy to centrally automate economic decision making (where IoT devices feed data into a central pool), or it can facilitate a more decentralised market driven economy where IoT devices create data as a privately owned and tradable economic asset. Current legislative and regulatory settings in Australia align more closely with a centralised model, which has advantages for governments but may hamper the entrepreneurial development of a competitive market economy. Further economic analysis assessing this potential institutional–technological trade-off would be useful to assess the different pathways that IoT adoption might bring.

1.6.3 Number of devices

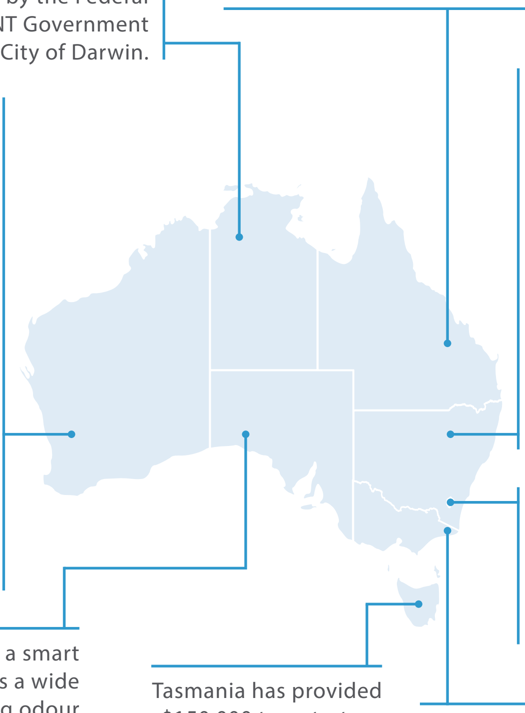
Research on the number and nature of IoT devices in Australia is an area for further research recommended by this report. However, industry estimates suggest that there are 16 million IoT connected devices installed in Australia in 2018–19 (Australian Communications and Media Authority, 2020a). As of May 2019, 50 percent of Australian adults used a smart device (other than a computer, tablet or mobile phone) connected to the internet (Australian Communications and Media Authority, 2020a). The average household is predicted to have 18 connected IoT devices by 2023 (Telsyte, 2019). In addition, consultancy firm Ovum has forecast that more than 47 million smart devices will be installed in Australian homes by 2022, a 295 percent increase on 2019 figures (Australian Communications and Media Authority, 2020a).

1.6.4 National IoT initiatives

While it is difficult to quantify the initiatives that are occurring in this rapidly developing space, some of the key initiatives in Australia at the time of writing of this report are detailed below.

- The Australian Government's $50 million Smart Cities and Suburbs Program was announced in 2016, which funded 81 collaborative smart city projects, to improve the liveability, productivity and sustainability of Australian cities, suburbs and towns. There were two funding rounds in 2017 and 2018.

- Projects have included the building of digital infrastructure, installation of sensors connected to IoT platforms to support better understanding of environments to facilitate better community engagement, service delivery and planning. In addition, a number of partnerships between the three levels of government across seven cities to create productive and liveable cities have also supported the development of IoT initiatives.
- The national peak-body Internet of Things Alliance Australia (IoTAA) was formed in July 2016 to represent industry interests in the IoT. They currently consist of 500 participating organisations and 1,000 individuals. They have released several standards and guidelines including the IoT Reference Framework, the IoT Platform Selection Guideline and Good Data Guide to support knowledge and standardisation across industry.



Queensland Government is to invest $3 million into IoT pedestrian crossings with sensors to detect pedestrian movement and adjust the time required to cross. The investment will support a roll-out of up to 300 smart crossings over the next two years.

NT Government has contributed $2.5 million to a $200 million Darwin City Deal to support their smart city initiative, jointly funded by the Federal Government, NT Government and the City of Darwin.

As part of the IoT DecisionAg Grant Program, the WA government awarded 15 grants to 8 grower groups and 5 agricultural schools/colleges to investigate different on-farm connectivity solutions and technologies (in particular, Low Power Wide Area Networks (LPWAN) using the LoRaWAN and SigFox communication protocols, and higher bandwidth using 3G/4G mobile networks, mesh and on-farm Wi-Fi networks) to support remote on-farm monitoring using IoT and data analysis platforms.

Transport for NSW has made recent developments to use IoT sensors to collect real-time information about passenger train journeys. The data includes a snapshot of how full a particular carriage is through travel apps and is also being used by Downer EDI Limited, who maintains Sydney's trains, to generate insights that may be able to enable predictive maintenance in the future.

ACT replaced 45,000 streetlights in its network with LED technology, which allowed real-time monitoring to automatically detect failures.

SA Water has trialed a smart wastewater network that uses a wide variety of sensors (including odour and overflow pattern sensors, weather stations, air pressure and flow direction sensors) linked to cloud-based data analysis to provide real-time information on the SA water network to manage overflow and odours.

Tasmania has provided $150,000 to a start-up accelerator run by EnergyLab, focused on hardware IoT solutions for the clean energy sector.

Victoria began a $3.5 million trial to connect cars on metropolitan and regional roads to speed limit and traffic light data for the first time. The trial was the first local use of 5.9GHz radios based on 4G Cellular V2X technology, which allows cars to communicate without using the mobile cellular network.

Figure 5: State specific IoT initiatives

- The Industry 4.0 Advanced Manufacturing Forum succeeds the Prime Minister's Industry 4.0 Taskforce. It builds on the work of the Taskforce in promoting collaboration between government and industry in Germany and Australia on Industry 4.0, including initiating a collaborative approach to the development of global Industry 4.0 standards. It will oversee the creation of six national Industry 4.0 Testlabs, due to be completed in 2020, which will showcase an immersive approach to advanced manufacturing.
- The Australian Government is developing Australia's 2020 Cyber Security Strategy. To complement the proposed strategy, a proposed voluntary *Code of Practice: Securing the Internet of Things for Consumers* has been released for public consultation.
- The Australian Competition and Consumer Commission's (ACCC) 2017 Digital Platforms Inquiry recognised a number of challenges posed by IoT devices.
- The Consumer Data Right, which commenced in early 2020, is intended to provide a right for consumers to require data portability from commercial entities in order to 'improve consumer control over the data which businesses hold about them'. The right has been introduced to the banking sector first, with the energy and telecommunication sectors to follow. This is proposed to be followed by other sectors over time.

1.7 Social and cultural developments

Limited research has been conducted on how Australians are engaging with the IoT technologies available to them. Peak bodies consulted as part of the consultation phase of this report suggest that the use of smart devices by the Australian public is expanding, but the term 'Internet of Things' is still not commonly understood. Representatives from the ACMA, the Australian Communications Consumer Action Network and CHOICE, an Australian consumers' organisation, indicate that issues such as personal data collection and use, privacy and security remain secondary, with customers choosing to buy IoT devices for convenience and functionality. According to the Australian Communications Consumer Action Network, Australians are gradually becoming aware of new IoT devices that are coming onto the market, but their awareness of the potential impacts of these technologies is more limited.

The CHOICE representative argued that most Australians have not yet been exposed to mass media coverage about the IoT, let alone about the significant risks related to IoT devices. It is difficult for consumers to identify how IoT devices such as smart home security systems, smart toys or digital assistants are generating and using personal data. If there had been local incidents of vulnerable groups, such as children, being adversely affected by these technologies, Australians would possibly be more cautious about IoT technologies.

These agencies suggested that better consumer consultation and consumer design-led initiatives need to be established in Australia. However, the lack of data about consumer understanding of the IoT and the rapid rate of change of these technologies makes the idea of consultation challenging.

These agencies, as well as representatives from Austroads and Intelligent Transport Systems (ITS) Australia, emphasised that access to reliable connectivity remains a problem for Australian consumers living in RRR areas; even some areas very close to major cities lack reliable connection to mobile phone networks or WiFi. Austroads representatives noted that more fatal vehicle accidents take place on rural roads than urban roads, and poor connectivity can hinder emergency services response times, increasing risk of lasting injury or damage to property. This means that it will also be difficult for smart transport and road safety systems to operate in these conditions. Key infrastructure is already lacking; for example, most roads are managed by resource-poor local councils and many Australian roads remain unsealed. Vast volumes of data are already generated by smart sensing and other digital data collection on Australian transport systems, but agencies are finding it challenging to make use of the data.

The Cairns Institute at James Cook University studied the connectivity and digital inclusion of agricultural communities in Far North Queensland (Marshall et al., 2019). The report found that basic infrastructure needed to support the uptake of novel technologies like the IoT was deficient in this region. The authors recommended that the Australian Government improve affordability and access to digital connectivity in RRR areas and provide targeted digital capability building and skills programs. Without these basic requirements being fulfilled, smart farming and other IoT services that can increase productivity may have little chance of success in RRR areas.

Very few studies exist of Australian consumers' use of existing IoT devices. One study involving Australian families who were early adopters of smart home technologies showed that participants often used smart home surveillance technologies to engage in caring remotely, by checking that children, family members with disabilities, or pets were safe and protected (Strengers et al., 2019).

1.8 Regulatory developments

The Australian Government has assessed the IoT as part of broader work on emerging technologies. The Productivity Commission's 2017 research report on data use and availability mentioned the increasing use of IoT devices as sources of data collection. It contained a case study which included some examples of IoT devices and described potential risks and challenges to successful deployment of these technologies. The ACCC's recent Digital Platforms Inquiry also recognised challenges posed by IoT devices. However, the wider impact of such technologies was still too unclear to form a foundation for specific recommendations to government, other than that policy-makers should 'actively engage with the implications of these developments when formulating policy and considering regulatory reform' (Australian Competition and Consumer Commission, 2019a, p. 518).

The Australian Government is developing their 2020 Cyber Security Strategy (Australian Government, 2019a). The Department of Home Affairs alongside the Australian Cyber Security Centre has also released a proposed voluntary code of practice for public consultation that recommends a set of measures for industry as the standard for IoT devices (Australian Government, 2019b) and to raise awareness in industry and, indirectly, with consumers.

Stakeholders across sectors noted key efforts on standardisation, including:

- The IoTAA has released two successive versions of an IoT Security Guideline (Internet of Things Alliance Australia, 2017b). They have also released a Good Data Guide, suggesting principles by which businesses should abide in dealing with consumers (Internet of Things Alliance Australia, 2017a).
- Standards Australia noted that they were actively participating in the ISO and the International Electrotechnical Commission's International Standards body, working with a national committee to develop a set of standards for application to Australia in the next 6–12 months. Standards Australia also released a Smart Cities Standards Roadmap in August 2020, with recommendations for Australian governments and industry to support the ongoing development of smart cities and communities in Australia.
- Austroads indicated that the National Transport Commission and state and territory governments have been assessing the deployment of CAVs, including guidelines for trials in Australia. However, the mobility sector will face specific challenges with interoperability, given that most vehicles in Australia are exported from overseas. Ideally, standards should be coordinated at a national level to ensure vehicles can operate across different jurisdictions.
- The Commonwealth Scientific and Industrial Research Organisation (CSIRO) and IBM Research considered that the required standards were already in place for the health sector and further work was not necessarily needed. In fact, revised standards for the health sector could damage the nuance and sophistication of the current system. Stakeholders suggested that future directions should focus on integrating the IoT with existing records, technologies and behaviours.
- CHOICE noted that Australia already has very good consumer legal protection by international standards. It can build on this in relation to IoT technologies, as consumer laws are framed in general terms and are therefore applicable to many new consumer goods and services.
- In terms of telecommunications regulation, the ACMA noted that developments in IoT technologies have been successfully encompassed within existing regulatory arrangements across its regulatory remit, with regulatory settings to be readjusted as needed. ACMA also released an Internet of Things Occasional Paper in August 2020 exploring the impacts of IoT across media and communications.

CHAPTER 2
APPLICATIONS OF THE IOT IN SMART CITIES AND REGIONS

Chapter overview

Short-term

- Key sectors where IoT is forecast to have high impact in the short term include service delivery, advanced manufacturing/ Industry 4.0 and health service delivery.
- IoT systems are becoming more integral to the delivery of services by supporting the integration of real-time information services in the delivery of transport, urban planning, infrastructure and utilities management, and citizen engagement by governments at local, state and federal levels.
- Through artificial intelligence and predictive analytics tools, the IoT will enable smart infrastructure systems to help city managers monitor the performance of vital assets, identify key areas where city services are lagging, and inform decision makers on how to manage city growth and make our cities more liveable.
- There is a shift towards 'platform urbanism', whereby technology companies use advances in the IoT and data analytics to extend the reach of their existing platform ecosystems into urban domains.
- Future developments in IoT-based healthcare could use AI to assist and inform health professionals and enhance current diagnostic capability. To realise the potential of IoT-based healthcare and guide implementation in Australia, national bodies could consider developing a strategy that assesses IoT health applications from a clinical implementation perspective, outlines areas for further R&D and provides appropriate regulation for data management.

Medium-term

- Medium term applications of the IoT include smart mobility, freight and logistics, public service transformations, education and smart campuses, and in the creative industries: galleries, libraries, archives and museums (GLAM) sector.
- Smart mobility is forecast as one of the medium-term applications to improve mobility and public transport in cities and regions. This encompasses the use of technology and advanced algorithms to provide travellers with seamless and flexible trips across all modes of transport.

- IoT applications in freight and logistics include real-time tracking of shipments, warehouse-capacity optimisation, predictive asset maintenance and last-mile delivery, leading to improved operational efficiency, safety and security.
- The IoT has the potential to transform government service delivery by facilitating a more customer-centric approach through data integration. The capacity for transformative impacts may require a 'reinvention of governance' in government service delivery.
- GLAM IoT initiatives demonstrate the opportunities to use participatory exhibits to encourage citizen participation and interaction. Initiatives such as these could be used to improve data and digital literacy as the use of connected devices in society becomes more commonplace.
- Our increasing dependence on connectivity for essential services should be assessed as part of ongoing prevention and response to future disaster management. State emergency service departments could consider integrating emerging technologies, such as IoT, with their existing systems so that accurate and targeted information can be strategically deployed directly to local authorities.

Long-term

- Opportunities in the long-term include digital twins, novel data considerations from data captured from the IoT and enabling ubiquitous interfaces and augmented/virtual reality.
- It is predicted that the value of digital twins will rise exponentially over the next decade and eventually overtake the value of the manufacturing process equipment.
- Developments in real-time IoT data analytics are likely to lead to a research field in its own right with a plethora of dissemination and exploitation opportunities. It is expected that the IoT will increase the number of personally identifiable data flows. Data science techniques and provenance schemes will be useful in assisting to quantify the likely completeness, precision and accuracy of data records.
- Data integration is likely to provide opportunities in pervasive and augmented reality, where connected decision-interface technologies like glasses with visual, auditory and tactile augmentation capabilities linked to other mobile and wearable technology will make information access and interactions more ubiquitous and pervasive.

2.1 Introduction

This chapter focuses on applications that are likely to have scalable impact across cities and regions, highlighting the opportunities and challenges they present. Applications are divided across the following sections: cities and regions; cities/urban areas and regions. IoT will enable users to monitor and manage devices, systems and infrastructure remotely, and then analyse and act on the information received from various real-time data streams (Mohanty et al., 2016). Figure 6 shows a range of potential IoT applications over the next decade.

While the application of the IoT across cities and regions differs according to the requirements of a place, common goals can be achieved, such as sustainability, citizen wellbeing, optimisation of services, and economic and productivity gains (Figure 7).

A smart city can be defined as a city that (i) has connections between its physical, information, communications, social and business infrastructures, and (ii) has the potential to consolidate datasets and analyse these to optimise services. Smart city services need to be secure and trustworthy as well as scalable and efficient.

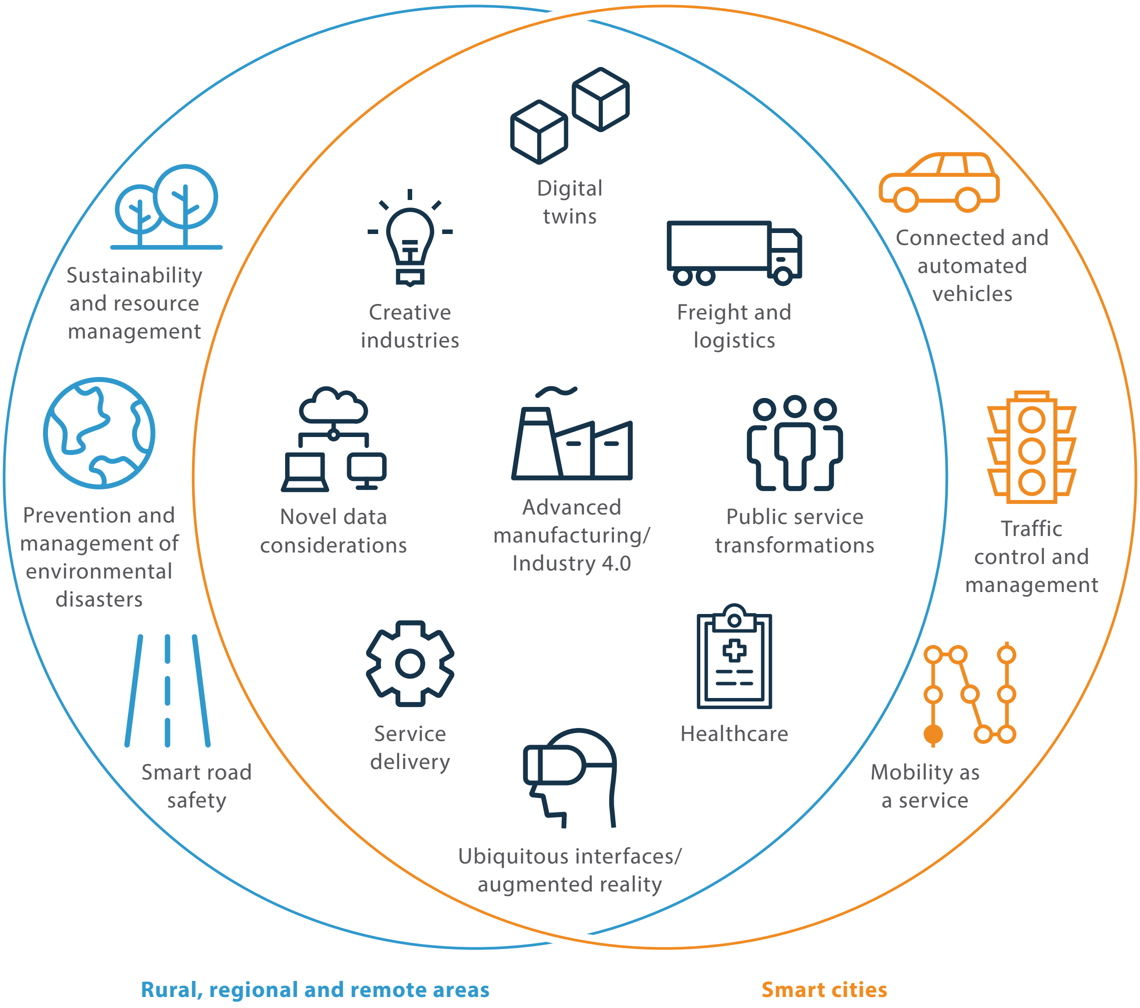
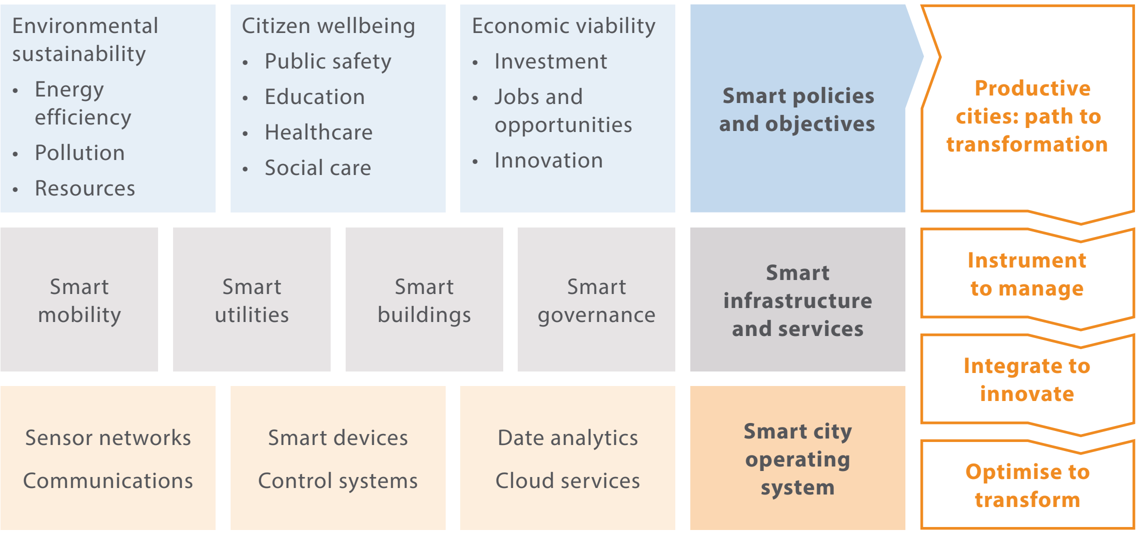

Digital twins
Creative industries
Freight and logistics
Connected and automated vehicles
Sustainability and resource management
Novel data considerations
Advanced manufacturing/ Industry 4.0
Public service transformations
Traffic control and management
Prevention and management of environmental disasters
Service delivery
Healthcare
Mobility as a service
Smart road safety
Ubiquitous interfaces/ augmented reality
Rural, regional and remote areas
Smart cities

Figure 6: IoT applications in smart cities and regions

Smart regions have similar requirements to cities but the IoT applications in regions are likely to be related to specific opportunities or challenges faced by that community. Key applications for the IoT in regions are likely to be agricultural (e.g. monitoring livestock and crops on farms)[16] and resource management (e.g. monitoring water and energy usage). During consultation with state and territory governments, it was suggested that while key IoT investments are likely to occur in cities, deployments in regional and remote areas may be of greater utility and value because the IoT can be used to optimise the use and management of limited resources for smaller communities. Mid-sized cities such as Newcastle, the Gold Coast and Wollongong have also seen significant investments to date. Local governments and the Australian Government have co-invested in initiatives through the Smart Cities and Suburbs Program.

As with all emerging technologies, the expected impact of the IoT across sectors is difficult to predict accurately. Additionally, changing market trends and customer preferences is likely to result in uneven impacts within sectors. However, categorising applications by anticipated impact can provide a useful baseline to guide investment and policy efforts by government and industry. We are already beginning to see the benefits of the IoT in service delivery, healthcare and Industry 4.0 or advanced manufacturing. In particular, many cities and local government areas have begun implementing IoT solutions to track and monitor urban issues such as traffic congestion, waste management and community safety. Developments in IoT-enhanced healthcare have been driven by the recent emergence of COVID-19, and the need to improve patient-centred outcomes, track community transmission rates and reduce burden on hospitals. In Industry 4.0 there are opportunities for reshoring a domestic manufacturing sector by enabling agile and responsive production without a high labour cost. This could help make Australia globally competitive.



Environmental sustainability
- Energy efficiency
- Pollution
- Resources

Citizen wellbeing
- Public safety
- Education
- Healthcare
- Social care

Economic viability
- Investment
- Jobs and opportunities
- Innovation

Smart policies and objectives

Productive cities: path to transformation

Smart mobility

Smart utilities

Smart buildings

Smart governance

Smart infrastructure and services

Instrument to manage

Integrate to innovate

Sensor networks

Communications

Smart devices

Control systems

Date analytics

Cloud services

Smart city operating system

Optimise to transform

Figure 7: Smart infrastructure underpinned by digital innovations can help cities and regions to achieve their goals

Adapted from Dia et al., 2019.

[16] Refer to the ACOLA Report *The Future of Agricultural Technologies* (Lockie et al., 2020).

In the medium term, it is anticipated that the smart mobility sector, freight and logistics sector, public service, education and creative industries are likely to gain significant improvements and opportunities from the use of IoT. Accurate and real-time monitoring of public transport systems will enhance population mobility in urban areas with the use of sensors across assets, offering more freedom in choice and convenience for users. The freight and logistics industry also stands to gain considerable benefits from the integration of IoT across the entire supply chain including real-time tracking of shipments, warehouse-capacity optimisation, predictive asset maintenance and last-mile delivery. Transformations in the public service are likely to require a 'reinvention of governance', where the IoT will enable the extension of data analytics into more diverse dimensions of service delivery, facilitating a more customer-centric approach, reducing resource use, and improving regulatory compliance. In the education and the creative sector, the use of IoT will create dynamically responsive and tailored environments, such as improving classroom and campus environments or facilitating new ways to interact with museum or gallery collections and environments.

In the future, long-term applications include capitalising on the exponential quantities of data that will be captured from the IoT. This includes the development of digital twins, which will enable the creation of detailed and real-time digital representations of a physical asset to model its lifecycle and improve diagnostics and maintenance. Digital twins have been forecast to be more valuable than physical asset themselves. Novel ways to analyse and process data are likely to emerge, and will also support associated technologies such as augmented reality and ubiquitous interfaces.

2.2 IoT applications across cities and regions

The IoT is already providing benefits across cities and regions including service delivery, public service transformations and healthcare. In the next five to seven years, we expect integration of IoT into the education sector as well as the creative industries to improve engagement with students and community. Industries such as advanced manufacturing, freight and logistics are also expected to see productivity and efficiency gains, particularly with the advent of digital twins. Future areas for growth at the end of the decade include capturing value from vast amounts of data collected from IoT networks which may lead to new business models to process, verify and analyse data, and supplement associated technologies such as augmented reality and ubiquitous interfaces.

2.2.1 Service delivery

IoT systems are increasingly becoming integral to the delivery of services such as transport, urban planning, infrastructure and utilities management, and citizen engagement. In Australia, the implementation of the IoT has been accelerated through the Australian Government's Smart Cities and Suburbs Program. This initiative has made co-investments with local governments in smart city trials in domains such as smart parking, smart waste management, smart metering and digital engagement initiatives.

2.2.1.1 Predictive infrastructure management and monitoring

Infrastructure operators have used supervisory control and data acquisition systems to monitor, gather and process data in real-time for decades. IoT systems now offer opportunities to improve these systems through enhanced detection, prevention and maintenance. For city governments, the applications could be as diverse as the monitoring and management of traffic infrastructure, household utilities, crime and adaptation to climate change (e.g. through urban heat monitoring, tree canopy mapping, and flood management) (Kamilaris and Ostermann, 2018).

Sensors in urban environments communicate with each other to enhance infrastructure capability and resilience. This dramatically lowers the cost of deployment and operation of data collection, management and analysis. It also enables automated and finely grained monitoring of asset utilisation to better predict and plan for capital expenditure and lifecycle costs (Manyika et al., 2015). Through AI and predictive analytics tools, smart infrastructure systems can help city managers monitor the performance of vital assets, identify areas where city services are lagging, manage city growth and make our cities more liveable. For example, IoT systems can be used to detect vulnerabilities or faults in assets to prevent major interruptions to services that can be costly and disruptive. This also means there is higher resource utilisation and reduced capital and operational costs. Other potential applications of the IoT include the use of digital dashboards by local governments to capture functions of urban services, including traffic incidents, planning and property approvals, and the health and maintenance of street trees.

City of Newcastle's depiction of a smart city zone (Figure 8) demonstrates the seamless integration of sensors into a connected network that enhances public spaces and service delivery.

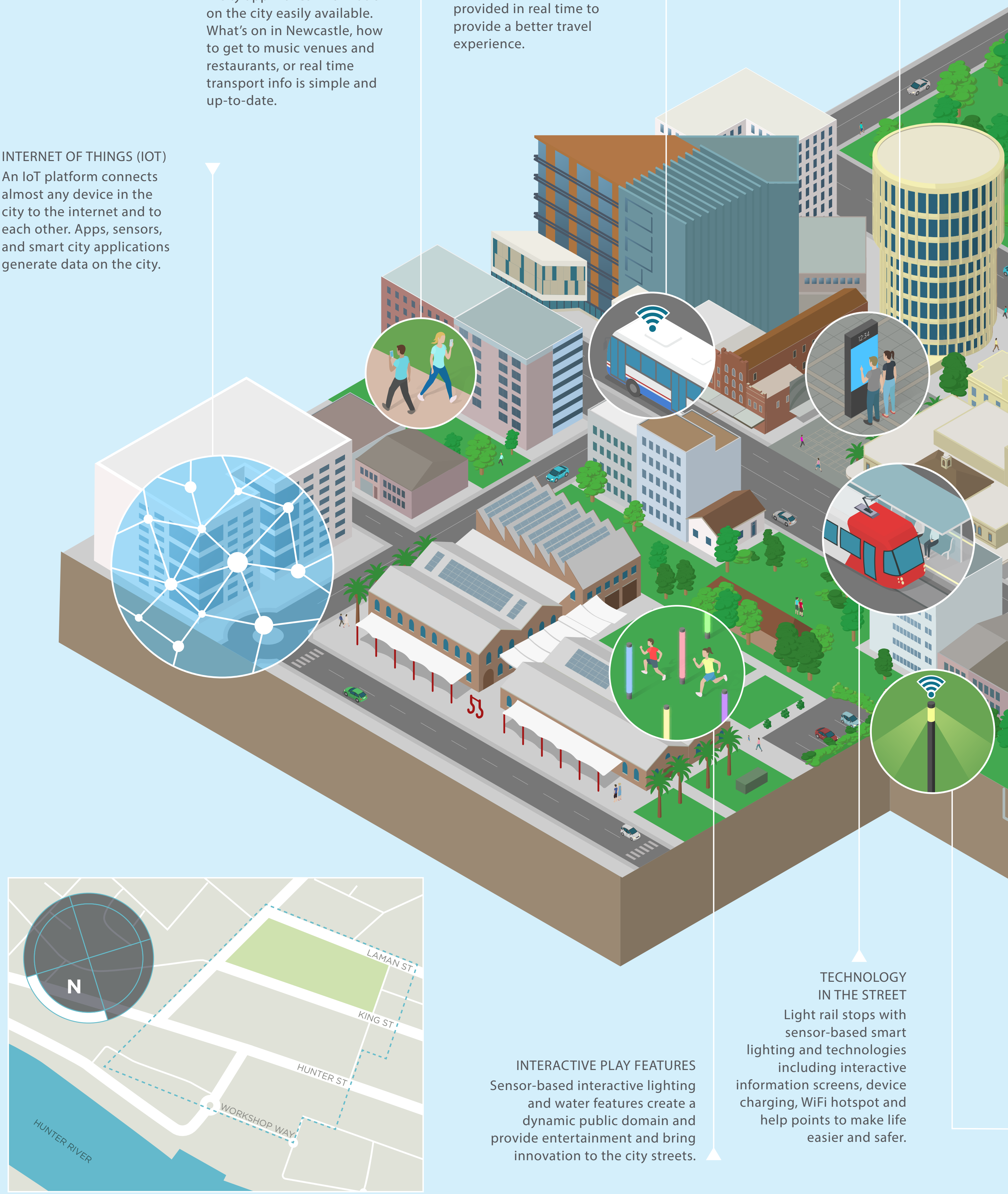
2.2.1.2 Predictive management of road infrastructure

Poor maintenance of infrastructure can be costly and may result in damage, including, in the case of roads, risk to driver safety (Mednis et al., 2011). IoT offers opportunities to fundamentally transform the way our transport infrastructure is maintained. For example, sensors that monitor the structural integrity of bridges have proved to be effective in identifying maintenance needs, which helps to ensure safety for travellers (Kurata et al., 2012). Road condition monitoring has also been proposed in New South Wales (NSW) and trials have shown detection of 97.5 percent of road damage (Anaissi et al., 2019). Deep learning techniques can be used to improve the accuracy of data collected from sensors for the automatic detection of different road surface conditions, with the results showing high detection accuracy (Varona et al., 2019). Advances in this space will allow for the creation of digital simulation models by integrating IoT, AI, data analytics and machine learning.

In RRR areas, predictive maintenance enabled by IoT is particularly useful as road and transport infrastructure can be challenging to maintain, requiring high cost and manpower where roads are particularly remote (see, for example, Cardinia Shire Council, 2019). Regular data feedback on the quality of infrastructure, with alerts sent when repairs are required, would optimise existing processes, streamlining roadwork maintenance schedules and reducing costs for local governments. A focus on high-reliability, low-power, solar-based systems that require minimal installation should be considered.

Figure 8: City of Newcastle's prospect for a future Smart City

Adapted from City of Newcastle, 2017.



SMART SCREENS

Interactive smart screens around the CBD provide information to help people find out the latest on what's going on in the city.

SMART MOBILITY

All forms of transport are linked together to make getting around simple and seamless. Timetables are synced and vehicle locations provided in real time to provide a better travel experience.

SMART CITY APP

A city app makes information on the city easily available. What's on in Newcastle, how to get to music venues and restaurants, or real time transport info is simple and up-to-date.

INTERNET OF THINGS (IOT)

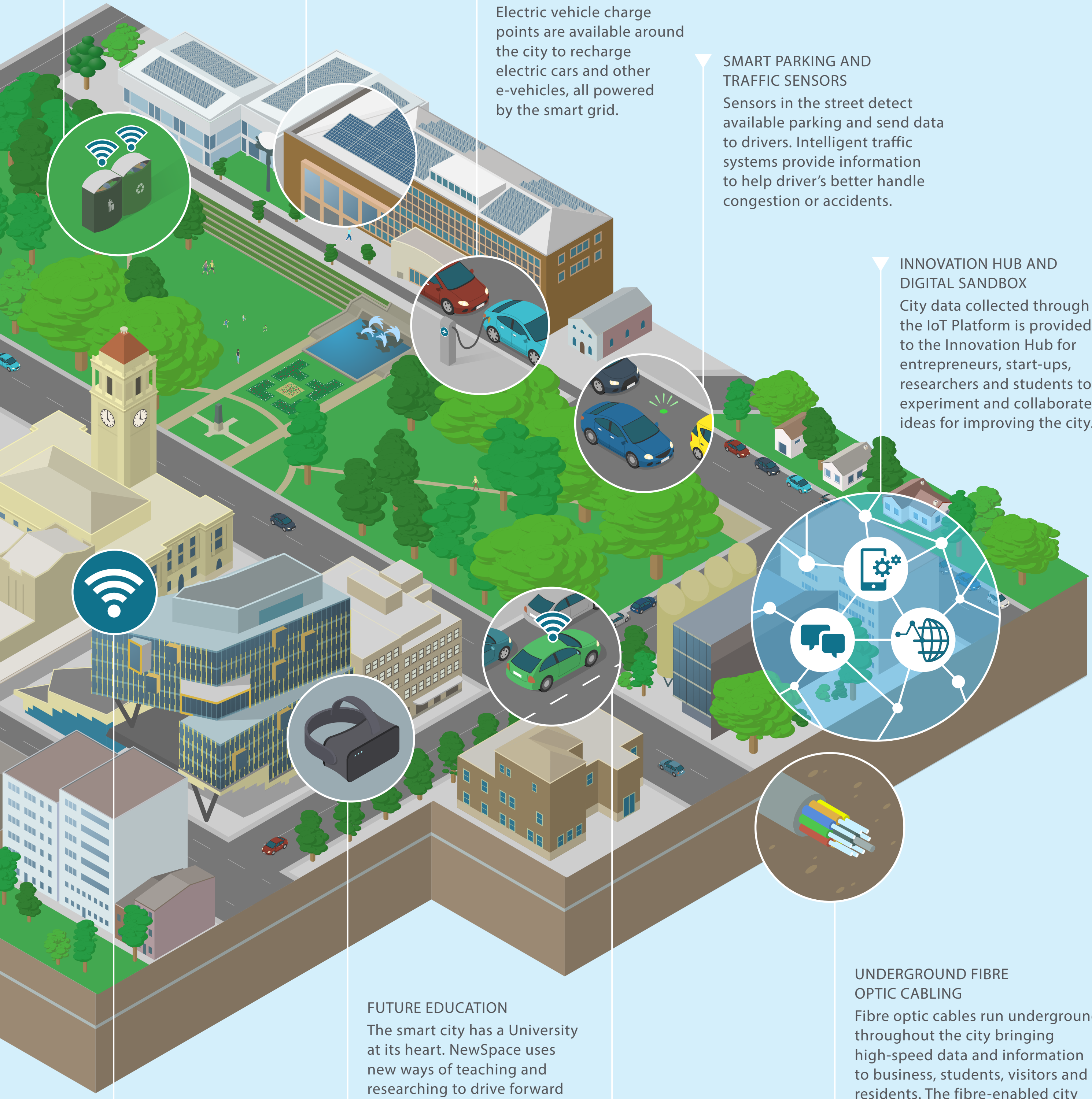
An IoT platform connects almost any device in the city to the internet and to each other. Apps, sensors, and smart city applications generate data on the city.

TECHNOLOGY IN THE STREET

Light rail stops with sensor-based smart lighting and technologies including interactive information screens, device charging, WiFi hotspot and help points to make life easier and safer.

INTERACTIVE PLAY FEATURES

Sensor-based interactive lighting and water features create a dynamic public domain and provide entertainment and bring innovation to the city streets.



SMART BINS

Sensors linked to the IoT platform collect data on the city and transform everyday items into smart infrastructure. Bin sensors will detect when bins are full and optimise collection routes.

SMART ENERGY

Buildings are powered by the sun through solar panels connected to battery storage.

ELECTRIC VEHICLE CHARGE POINTS

Electric vehicle charge points are available around the city to recharge electric cars and other e-vehicles, all powered by the smart grid.

SMART PARKING AND TRAFFIC SENSORS

Sensors in the street detect available parking and send data to drivers. Intelligent traffic systems provide information to help driver's better handle congestion or accidents.

INNOVATION HUB AND DIGITAL SANDBOX

City data collected through the IoT Platform is provided to the Innovation Hub for entrepreneurs, start-ups, researchers and students to experiment and collaborate on ideas for improving the city.

FUTURE EDUCATION

The smart city has a University at its heart. NewSpace uses new ways of teaching and researching to drive forward our thinking about the challenges of the future.

PUBLIC WIFI

Free public WiFi is available providing high speed quality internet access no matter where you are in the CBD.

UNDERGROUND FIBRE OPTIC CABLING

Fibre optic cables run underground throughout the city bringing high-speed data and information to business, students, visitors and residents. The fibre-enabled city is attractive and more liveable.

SMART PARKING APP

A smart parking app will guide drivers quickly to the best available parking spot near their destination; pay by phone and top up remotely.

SMART LIGHTING

Smart poles provide energy efficient LED lighting, but that's not all. Each pole can house WiFi signal points, sensors, public address system and more.

This is an indicative illustration only

2.2.1.3 Resource and utility management

The potential for future energy and water insecurity calls for better allocation and management of existing resources. IoT sensors and distributed systems can optimise consumption and resource allocation (Mohanty et al., 2016). Smart sensors can assist in early detection of risks and faults reducing the need for future, more costly repairs, while smart meters record consumption and relay that information for monitoring and billing, facilitating accurate and reliable readings with minimal intervention. This can assist users to track consumption and make more informed choices. This results in more efficient, integrated, economical and more sustainable systems, with lower levels of resource loss, higher-quality supply and increased safety of systems and users (Mohanty et al., 2016).

Energy management

The IoT presents a major opportunity in energy management for cities and regions. Australia's electricity grid is rapidly transitioning to a two-way system in which energy consumers are also producers, or 'prosumers'. The 'future grid' enabled by the IoT could include:

- 'smart grid' technology, which uses IoT devices to ensure an energy grid can more responsively react to local changes in energy use and supply.[17] This will include technologies such as rooftop solar photovoltaic systems, battery storage, automated control of hot water systems and pool pumps, and smart or IoT-enabled appliances and air conditioning
- increased capture of renewable energy (solar, wind, hydrogen) by providing real-time responses to the natural fluctuations in generation, and to enable allocation at specified voltage and frequencies
- demand response programs that ask households and businesses to vary the timing of their consumption in response to variable pricing, incentives, rewards or other appeals
- community-scale projects such as micro-grids
- a two-sided energy market involving third-party platforms and vendors, such as demand response aggregation and peer-to-peer trading.

Existing and future IoT applications allow consumers to spread their energy use more evenly, for example, by installing technologies which automate usage ('set and forget') or by agreeing to external monitoring and control of their energy production, storage and appliances for increased visibility and decision making. The IoT will also allow consumers to more effectively capture and share energy back into the grid. This future grid would involve a two-way system of energy production and use, increasing distributed energy resources. These moves will feed into existing possibilities for balancing energy supply and demand to the population, including technologies such as solar photovoltaic systems, smart appliances and micro-grids.

[17] This is sometimes described as the 'Internet of Energy' (IoE). IoE sensors optimise the efficiency of energy infrastructure, reduce wastage and have various applications, such as power monitoring and demand-side energy management. For example, a consumer device such as a washing machine could, when connected to the internet, only operate when there is sufficient energy from solar power. IoE also helps power companies generate energy based on demand, thus reducing wastage.

For RRR communities, the IoT may help to conserve energy resources, particularly as regional communities pay higher costs for energy and are far more likely to be adversely impacted by extreme weather events compared to urban areas (The Climate Council, 2016).

Water management

With high water allocation prices expected to continue and the risk of droughts (Westwood et al., 2019), usage, resource-sharing and recycling practices will require greater visibility across homes, precincts and buildings. Water conservation management can be enhanced through early detection of leaks in pipes using sensors, as well as through the provision of more data to consumers so that they can track water usage and costs.

Case study 1: Smart customer water monitoring

The Goldfields Water County Council's app, MyH20, enables consumers to access hourly water usage, set consumption targets and receive alerts (including detected leaks) via their smart phone in conjunction with existing smart water meter reading technology. This will help minimise costly bills and help reduce consumption. This project was funded under the Australian Government's Smart Cities and Suburbs Program.

Case study 2: Innovation in water management practices

Pooled Energy is a start-up that bundles pool cleaning management with optimised energy supply, using a pool automation unit that connects to an existing pool pump. Information on the electricity market, grid and weather information, as well as swimming activity, is analysed to calculate the most cost-efficient time to run pool equipment (Pooled Energy, 2020).

Waste management

There have already been efficiency improvements in waste management through the use of smart bins in Newcastle and Melbourne (City of Melbourne, 2016; Intouch Magazine, 2019). Sensors in smart public bins monitor waste levels and, when bins are full, report to waste management services to facilitate efficient removal. The Melbourne City Council noted that average weekly collections had been reduced from eight times a day to once a day (City of Melbourne, 2016). As the technology improves, and more data are collected, there will be opportunities to obtain more nuanced data to further optimise service delivery. Northern Beaches City Council, NSW, is testing 'crushing' bins that compact waste in places where traffic is high and which are not easily accessible by garbage trucks, for example, at Shelley Beach in Manly (Riches, 2019). In the future, alternative data streams such as traffic and weather data could be integrated to further optimise waste disposal routes.

The IoT may also be able to optimise recycling processes, by using sensors to separate specific materials at the time of collection. Investigations into low cost IoT technologies to support these types of use cases are nascent, but hold promise. Over time these technologies could enable very specific and targeted selection of waste and may enable the development of new products based on recycled materials. During consultation, an IoTAA representative noted that Canterbury Bankstown Council, NSW, is currently investigating the possibility of council garbage trucks identifying, and possibly even sorting, household recyclable garbage. Support and investment by governments could drive innovation in this sector, providing novel ways to manage waste, as well as creating new employment opportunities.

2.2.1.4 Public safety and emergency management

IoT has high utility in public safety and emergency management. Tangible benefits of these applications include: enhanced situational awareness at command centres, the ability to manage applications remotely and safely, and greater protection and oversight of first responders (European Telecommunications Standards Institute, 2019). This domain is expected to evolve from one of critical communications to 'critical intelligence'. Use case examples include: automatic fire detection systems in buildings and industry; monitoring of chemical, biological, radiological and nuclear air and water pollutants; emergency road management, surveillance systems for early detection of environmental disasters such as bushfires or flooding, and wearables to monitor personal safety and bio-vitals of first responders (European Telecommunications Standards Institute, 2019). The success of IoT systems for public safety and emergency management will depend on accuracy, reliability and ensuring redundancies are in place, to prevent potential failure conditions. This could include notifications to report low battery of devices or disrupted connectivity. Regulatory protections to preserve privacy and security will also be a critical factor in enabling public trust and confidence in these systems (European Telecommunications Standards Institute, 2019).

2.2.1.5 On-demand public transport

Provision of high-quality public transport services is one of the most effective ways to provide mobility services to match expected population growth, and to maximise existing road infrastructure, particularly in major cities (Figure 9). Conventional public transport systems operate according to a timetable on fixed routes, as this is most cost-effective for operators in urban areas during peak times, due to maximum vehicle utilisation (Transport NSW, 2020). However, services are usually reduced during off-peak periods and in low-density areas due to lower demands, leading to poor performance and reduced traveller satisfaction (Liyanage et al., 2019).

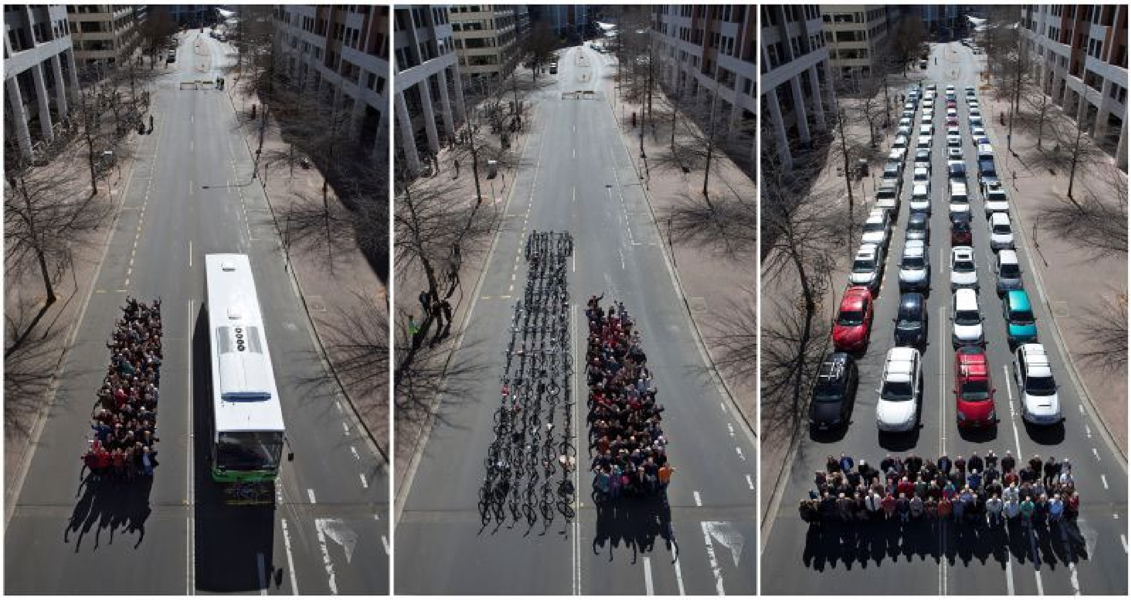


Figure 9: Space requirements for different modes of transport

Source: We Ride Australia, 2018.

On-demand public transport based on IoT technology is an attractive option to improve public transport services (Chong et al., 2012; Spieser et al., 2014), where access to real-time analysis of traffic and weather conditions (Burrows and Bradburn, 2014) and origin–destination demand can provide users with a more convenient, efficient, reliable and safe service (Ion et al., 2017; Liu and Ceder, 2015; Ma et al., 2017; Rosin, 2018). In addition, reductions in passenger wait time and travel time result in increased satisfaction and personal security (Brakewood and Watkins, 2018; Zhang et al., 2011; Zografos et al., 2008). It is estimated that reducing commuter buffer time could provide time savings equivalent to more than $60 billion per year (Manyika et al., 2015). Current examples include an on-demand mini-bus service in Sydney (Transport NSW, 2020).

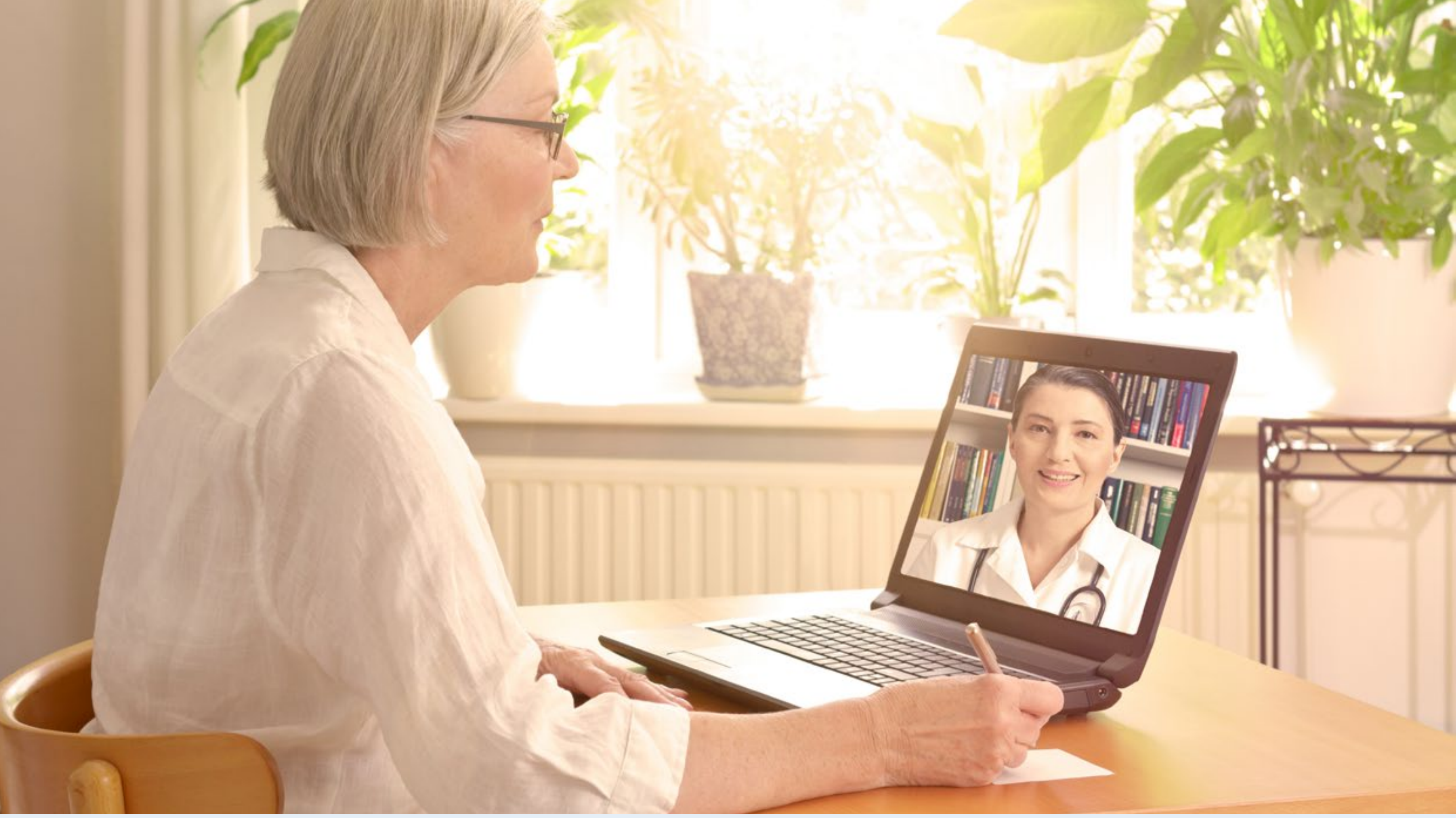
2.2.2 Healthcare

The potential of IoT is growing in healthcare and these developments provide great opportunity for healthcare systems to proactively predict health issues, diagnose, treat and monitor patients both in- and out-of-hospital. Cloud-based computing allows smart devices to collect information through sensing systems, in the form of medical devices, medications, activity trackers, and vital sign wearables, to remotely store this information, which can enable complex data analysis and AI-driven health decisions.

2.2.2.1 Smart connected healthcare systems

Smart connected healthcare systems offer the opportunity to improve IT systems currently used in healthcare, as well as integrate IoT devices to complement health service delivery (Sundaravadivel et al., 2018). Australia is in a unique position in its opportunity for growth in technology-assisted healthcare, transitioning from paper records to electronic patient records and other ICT health systems, into a single integrated system. This can provide health professionals and patients with greater insight into disease trajectories and outcomes, interventions and readmissions, as well as improved healthcare planning and budget allocations.

My Health Record is a cloud-based system that is managed by patients to share information with their healthcare providers. A future strategy integrating the use of the IoT could be to link data from health wearables to *My Health Record* to allow patients to view analysis of health risks, patterns and advice, all derived from IoT-based healthcare. Such initiatives will require a high degree of trust that data entered into a system like *My Health Record* are protected from illegal access or inadvertent breaches due to human error. For example, many Australians have opted out of having a *My Health Record* automatically created for them due to ongoing concerns about data privacy and security. However, developing analytical methods to harness the data being generated from integrated digital health records will be a particular challenge, as are interoperability and data storage solutions. For example, the Princess Alexandra Hospital in Brisbane, which has integrated EMR, generates more than 1 million 'atomised' data points daily.



Scenario 2: Smart healthcare

Mrs Rushmore is five minutes late for her doctor's appointment, as her smart watch reminds her for the fourth time. Luckily, it will only take her two minutes to get to the medical clinic situated in the residential facility where she lives. Her doctor, Dr Clements, is based in Sydney but has a telehealth practice that allowed Mrs Rushmore to stay on as a patient after she moved back to northern Queensland to be closer to her family. One of the nurses, who has also trained in information technology, assists Mrs Rushmore into the video-conference booth and settles her in.

Dr Clements is also running a little late, so Mrs Rushmore has time to look at her patient statistics. These are determined by a number of devices she always carries that send data to her phone. The statistics are also shared securely with her doctor. Her watch monitors her heart rate, blood pressure and exercise levels. Her blood sugar is checked by another device to help monitor her Type II diabetes. Everything seems fine, although her blood sugar levels are a little low. The device samples blood and measures blood glucose and can be used to inform her regular insulin injections. She checks the last reading, which was sent to Dr Clements practice's secure server 15 minutes ago. Her patient data is sent every half hour, so Dr Clements is able to monitor Mrs Rushmore's statistics in real time. Mrs Rushmore likes these devices because they have made things a lot more convenient for her. She also likes the fact that they will send an immediate alert to emergency services and to Dr Clements if they detect any significant discrepancies in Mrs Rushmore's vitals.

Dr Clements comes online and reviews Mrs Rushmore's statistics, which have been handily analysed and compiled into data charts. In reviewing the data, she thinks Mrs Rushmore might require a new medication for her blood pressure. She has been tracking the data and it seems that Mrs Rushmore's heart rate has been variable. She sends a quick note to the nurse on duty and the pharmacist at Mrs Rushmore's residential home to start her on the new course.

2.2.2.2 Smart health devices

IoT devices with applications for health and healthcare are being developed and include activity tracking devices, surgical devices, physiological monitoring devices and mobile phone apps. Sensing technologies allow for treatments to be monitored in real-time and physiological parameters about a patient to be acquired, so that diagnosis and high-quality treatment can be fast-tracked. The careful design and utility of sensing technologies can allow for continual data acquisition from patients with minimal disruption to the daily routine, facilitating the improvement of treatment outcomes and the reduction of healthcare costs (Dang et al., 2019).

Wearable smart devices allow data from wearable sensors to be connected with the cloud through Bluetooth, WiFi or GSM (Global System for Mobile Communications) (Bhatt and Bhatt, 2017). While wearable devices are becoming more prevalent and diverse in a demanding market, an important consideration will be their utility and wider role in an IoT-based healthcare system.

While the market for smart health devices is growing, not all are clinically tested or proven to be safe and effective. The Therapeutic Goods Administration is responsible for the regulation of medical and health devices in Australia. Ensuring that IoT devices are clinically proven and efficacious is essential to their availability and uptake by healthcare systems.

2.2.2.3 Primary (preventive) healthcare

IoT-based healthcare has the potential to assist in the primary intervention of many preventable diseases and improve population health (Australian Institute of Health and Welfare, 2019). However, it is important to note that there is currently a lack of evidence underpinning the majority of health apps on the open market to support these types of initiatives (James et al., 2018). Future applications of IoT-based healthcare should harness outcomes and learnings from apps that have been designed and developed from a strong evidence base.

2.2.2.4 Secondary and tertiary healthcare

An IoT-based healthcare system enables transition from a traditional model of service delivery which can be reactive, intermittent and sometimes uncoordinated to a more proactive, continuous and coordinated approach. Future applications of IoT-based healthcare could connect the patient and their care provider for treatment or monitoring outside of the hospital and in the patient's home, reducing health spending and improving the delivery of patient-centred care, through wearables and other interactive devices. Current examples include continuous glucose monitoring for people with diabetes on insulin pumps (N. Cohen, 2015) and remote monitoring of implanted cardiac devices (Queensland Cardiovascular Group, 2017).

Case study 3: Smart medications

Digital (or smart) medications typically consist of an ingestible sensor which communicates with an external body sensor such as a wearable patch (Plowman et al., 2018).The patch detects the signals from the ingested sensor and wirelessly communicates data to a mobile app or web portal (patient or provider). Information is stored in the cloud and is used to evaluate medication adherence and absorption and to measure activity and heart rate. The ultimate goal of digital medications is to improve clinical outcomes through better patient self-care, enhanced patient–provider dialogue and data-driven optimisation of therapy (Frias et al., 2017; Naik et al., 2017).

IoT-based healthcare could also encourage self-monitoring and data-driven health decisions and encourage people to seek health support when they need it through alerts and feedback. It may also provide the patient with information on when, where and who to seek professional health advice from (Korzun, 2017). IoT-based healthcare could also encourage self-monitoring and data-driven health decisions, regardless of location.

Research on costs and benefits of these initiatives is still emerging but overall health expenditure has been shown to be reduced by decreasing staffing and time in clinics, with time and financial costs associated with device set up and operation shifting to industry (Wilsmore and Leitch, 2017). Furthermore, costs are likely to be reduced as these applications become more ubiquitous. Future developments in IoT-based healthcare could also use AI to assist and inform health professionals and enhance current diagnostic capability.

2.2.2.5 RRR health service delivery

Mobile health and electronic health are examples of telehealth initiatives that use technology such as mobile phones and tablets to deliver care programs. These programs are flexible in time and location, with the potential to offer intensive interventions that may not be feasible with traditional care models. Some of these programs are slowly being adopted into clinical systems in Australia (Goode et al., 2013; Khanal et al., 2016). These initiatives may be particularly attractive to patients in RRR areas who have limited access to healthcare services.

There is currently limited research on the application of the IoT to telehealth in RRR areas. However, research to date highlights the adaptability and flexibility of the service model in response to needs as often being critical for success (Bradford et al., 2016). Remote patient monitoring will be advantageous for RRR areas, where cost and distance can limit access to high-quality patient centred care. This reduces costs to patients in these areas (especially reducing travel to health services and potentially moving to a care facility earlier than needed) and the health system.

While data issues, especially security and ownership (outlined in Chapter 3), will be of paramount concern to patients and service providers, it is clear that the IoT will supplement and optimise existing processes in telehealth for RRR communities. However, careful consideration will be needed in the implementation and resourcing of IoT health applications to address concerns from all stakeholders, especially given the vulnerable nature of some health users.

Case study 4: Wearable devices to monitor mental health conditions

Digital phenotyping using smartphone sensors to passively monitor day-to-day behaviour has been used successfully to identify individuals with bipolar disorder at risk of relapse (Kakria et al., 2015). This has enabled early intervention to minimise symptoms and impact on quality of life. Significant further R&D is required, however, before such services are ready for clinical or public use, including ensuring the protection of these highly sensitive data (Tashjian et al., 2017).

2.2.2.6 COVID-19

As of August 2020, the COVID-19 pandemic has encouraged the development and maturation of a number of digital technologies including IoT, big-data analytics and AI that uses deep learning and blockchain technology (Ting et al., 2020). IoT use cases have proven to be highly interconnected with these technologies. IoT ecosystems enabling the real-time collection of data at scale have been used by AI and deep learning systems to understand trends, model risks and predict outcomes. This is enhanced by blockchain technology, integrating peer-to-peer networks to ensure that data can be copied in multiple physical locations, using modified algorithms to ensure it is secure and traceable.

The IoT has provided a platform that has enabled public-health agencies access to data for monitoring new cases, disease distribution by country and severity of disease (Ting et al., 2020). For example, Johns Hopkins University Center for Systems Science and Engineering has developed a tracking map to monitor global statistics of COVID-19 cases, using data collected from a range of data sources including the United States' Centers for Disease, Control and Prevention, the World Health Organization (WHO), and the Chinese Centre for Disease Control and Prevention (Ting et al., 2020).

Smart health devices have also been deployed to reduce physical contact, enforce quarantine by tracking people's movements, lower the risk of healthcare-associated infections, reduce the burden on hospitals and to relieve caregivers. For example, wearable medical sensors and smart thermometers have been used in China and Taiwan to provide continuous real-time monitoring and alerts when abnormal body temperature is detected (Koh, 2020a, 2020b).

Case study 5: Using smart wearables to enhance telehealth

Smart wearables are being used in conjunction with telehealth initiatives to support the prioritisation of cases by severity, thereby reducing the burden on the healthcare system. For example, the University of New England in NSW is trialling the use of pulse oximeters to monitor vital signs (including heart rate, temperature, oxygen saturation, blood pressure and breathing) of patients who are in isolation or quarantine, reducing the need for extended hospital stays. Patients who test positive for COVID-19 will be allocated to three groups, either hospital admittance, home monitoring for milder cases with risk factors, or telehealth check-ups for less at-risk patients staying in their own home. For patients being remotely monitored, real-time alerts will be sent to a Joint Virtual Care Centre. This centre will also support clinicians from Armidale and Tamworth and other externally based specialists to deliver telehealth services. The University of New England has noted that a New England Virtual Hospital Network will be developed in close partnership with Hunter New England Health to progress the regional network health system (University of New England, 2020).

While these new IoT technologies offer important ways to deal with the COVID-19 pandemic, the preservation of human rights needs to be carefully considered when implementing IoT measures that are directed at monitoring people's movements or contacts and restricting their freedom to enter public spaces in the interests of containing the spread of the coronavirus. The accuracy and reliability of algorithmic decision making in these initiatives will require ongoing responsive assessment.

2.2.3 Public service transformations

The breadth of IoT applications for government service delivery is significant, including health management and services, utilities and resource management, urban planning and traffic management. Outcomes to these applications include facilitating a more customer-centric approach, reducing resource use, and improving regulatory compliance.

However, the capacity for transformative impacts is linked as much to a 'reinvention of governance' around government as a platform (GaaP) models of service delivery, as it is to the integration of IoT technology. GaaP represents a model for digital transformation of public services. The 2017 Productivity Commission Inquiry on Data Availability and Use has stated that 'fundamental and systematic changes are needed to the way Australian governments, business and individuals handle data (Productivity Commission, 2017). These changes must be implemented before the applications of the IoT can have a real impact on public services. In particular, public agencies need to be empowered to incorporate a wider variety of data inputs and feedback loops (generated by more prolific connected devices) to inform decision making.

A model for how governments could better integrate and link more diverse data sources from the IoT into decision making is outlined by the Victorian Government's Data Reform Strategy (Victorian Government, 2018). Positioning the work of Victorian agencies as part of a wider data ecosystem, which includes both public and private organisations, the strategy identifies the need for linked data and data partnerships that include a 'data hub'. This creates opportunities to draw from different layers of the data ecosystem, as well as facilitating greater sharing of de-identified data.[18] Also integral to this approach is a re-evaluation of different points of service delivery, which are divided into 'person', 'place' and 'economy'.

Figure 10 shows the kinds of data being considered as part of the Victorian Government's Data Reform Strategy. It provides a useful schematic for understanding how the IoT has the potential to reshape government services. While the IoT facilitates the extension of data analytics into more diverse dimensions of service delivery, a re-evaluation of underlying infrastructures and protocols for sharing and using data across government agencies and jurisdictions is needed before major benefits can be realised. The new infrastructure must respond to the significance of data analytics in shaping wider models of service design. It also requires more ambitious adoption of GaaP frameworks that address citizen- and user-centric approaches to service design, which may require moving away from existing agency structures. The Victorian Government's Data Reform Strategy provides an example of work that could be extended to other jurisdictions.

Fit-for-purpose data governance models should also include consideration of the implications of data commercialisation and use (and data surveillance) being extended into home and broader urban management settings. Data commons and open data collaboratives (discussed in section 2.5.5.2) could be considered as an opportunity for government to role model good data governance and management.

[18] Different state and territory privacy laws apply to de-identified data and the Office of the Australian Information Commissioner also provides guidance on de-identification.

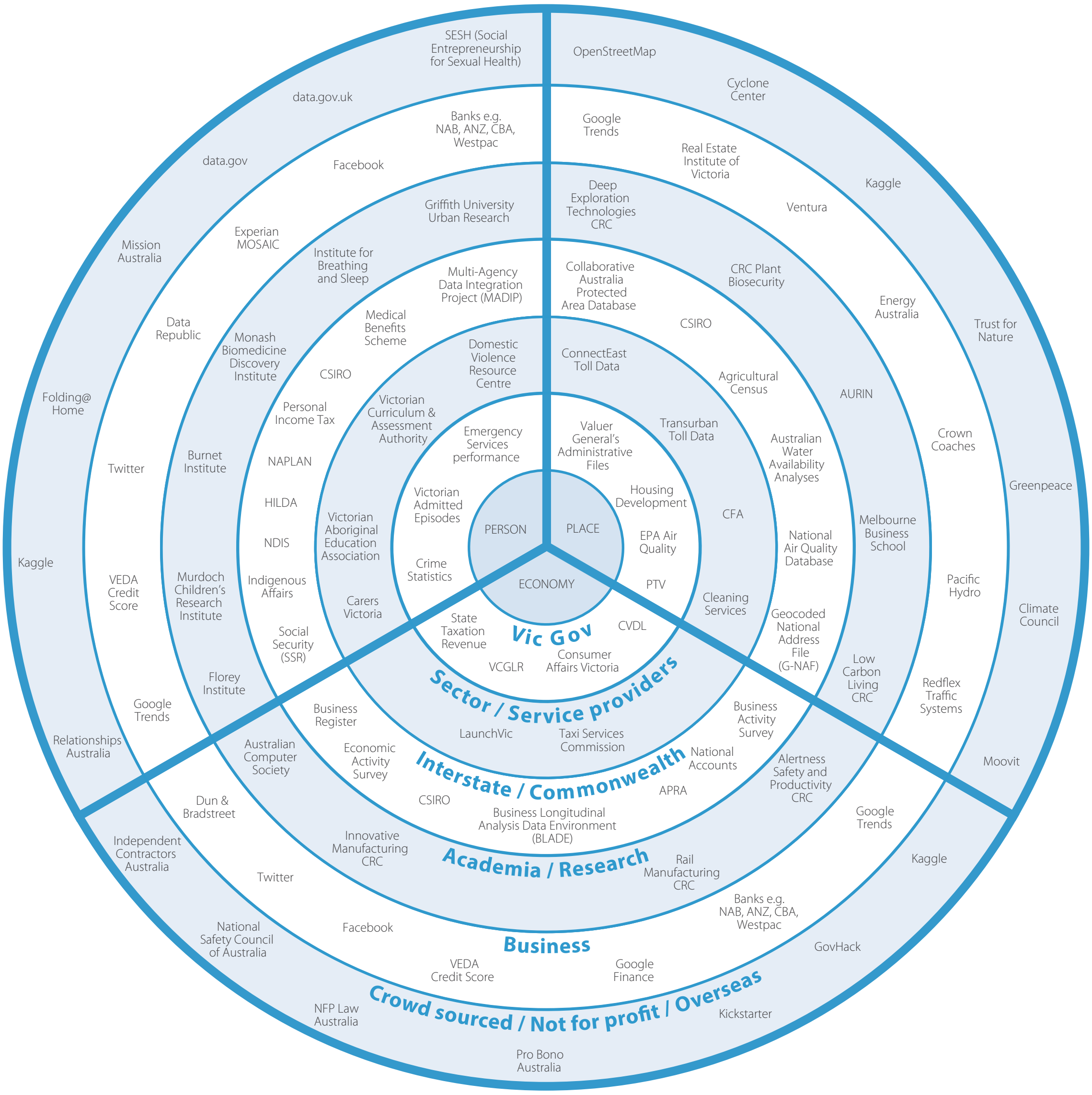

PERSON
PLACE
ECONOMY
Vic Gov
Sector / Service providers
Interstate / Commonwealth
Academia / Research
Business
Crowd sourced / Not for profit / Overseas
Victorian Admitted Episodes
Emergency Services performance
Valuer General's Administrative Files
Housing Development
EPA Air Quality
PTV
CVDL
Consumer Affairs Victoria
VCGLR
State Taxation Revenue
Crime Statistics
Domestic Violence Resource Centre
ConnectEast Toll Data
Transurban Toll Data
Victorian Curriculum & Assessment Authority
Victorian Aboriginal Education Association
Carers Victoria
CFA
Cleaning Services
LaunchVic
Taxi Services Commission
Multi-Agency Data Integration Project (MADIP)
Collaborative Australia Protected Area Database
Medical Benefits Scheme
CSIRO
Agricultural Census
Personal Income Tax
NAPLAN
HILDA
NDIS
Indigenous Affairs
Social Security (SSR)
Australian Water Availability Analyses
National Air Quality Database
Geocoded National Address File (G-NAF)
Business Register
Economic Activity Survey
CSIRO
Business Longitudinal Analysis Data Environment (BLADE)
APRA
National Accounts
Business Activity Survey
Griffith University Urban Research
Deep Exploration Technologies CRC
Institute for Breathing and Sleep
CRC Plant Biosecurity
Monash Biomedicine Discovery Institute
CSIRO
Burnet Institute
Murdoch Children's Research Institute
Florey Institute
AURIN
Melbourne Business School
Low Carbon Living CRC
Alertness Safety and Productivity CRC
Australian Computer Society
Innovative Manufacturing CRC
Rail Manufacturing CRC
Banks e.g. NAB, ANZ, CBA, Westpac
Facebook
Experian MOSAIC
Google Trends
Real Estate Institute of Victoria
Ventura
Energy Australia
Data Republic
Twitter
VEDA Credit Score
Google Trends
Dun & Bradstreet
Twitter
Facebook
VEDA Credit Score
Google Finance
Banks e.g. NAB, ANZ, CBA, Westpac
Google Trends
Crown Coaches
Pacific Hydro
Redflex Traffic Systems
SESH (Social Entrepreneurship for Sexual Health)
OpenStreetMap
Cyclone Center
data.gov.uk
data.gov
Kaggle
Mission Australia
Trust for Nature
Folding@ Home
Greenpeace
Kaggle
Climate Council
Relationships Australia
Moovit
Independent Contractors Australia
Kaggle
National Safety Council of Australia
GovHack
NFP Law Australia
Kickstarter
Pro Bono Australia

Figure 10: 'Smart infrastructure' framework underpinned by digital innovations

Adapted from Victorian Government, 2018.

2.2.3.1 Smart community engagement and education

The integration of the IoT in service delivery enables a more experimental and bottom-up approach to urban management and design. As a result, urban interventions and innovation initiatives, developed in 'urban living labs', and other temporary initiatives have emerged. For example, one of the first SENSEable City Lab projects, Real-time Copenhagen, used mobile devices to track people's movements through the city, displaying the pulse of Copenhagen's Kulturnatten (culture night) as it unfolded in real-time. These ideas were part of a wider movement that saw the potential for more ubiquitous technologies and sensors to facilitate a new kind of 'architecture of participation' in which traditional urban social structures and governance methods could be radically reconstituted. In more recent years, these experimental approaches have also been accompanied by citizen-sensing initiatives (Gabrys, 2014) and urban living labs. These have incorporated experimental uses of the IoT to explore the potential for improved data collection in areas such as water use, air quality monitoring, temperature mapping and citizen engagement (Bulkeley et al., 2016).

These experimental approaches to citizen science are also associated with the urban transitions movement, which seeks to accelerate the adoption of low-carbon and other urban sustainability initiatives. They offer ways in which the public can become involved in generating data that are relevant to their own concerns using IoT technologies, rather than just responding to top-down initiatives.

Case study 6: Student monitoring of environmental indicators

In a program launched by the City of Perth in August 2018, high school students partnered with universities and urban planners to examine how data sourced from IoT sensors can be used to facilitate new collaborations. Schools were offered the ability to monitor environmental indicators such as temperature, humidity, air and water quality in their local area and to collaborate with other participants to understand data about local environmental conditions. This project was funded by the Australian Government's Smart Cities and Suburbs Program.

2.2.4 Education and smart campuses

The IoT is being widely deployed across educational settings and university campuses, including some sites in Australia. In a sense, applications of the IoT in these environments are similar to those across smart cities – integrating more responsive, environmentally efficient lighting, improved campus security, and more granular understanding of campus foot traffic dynamics, classroom uses and parking issues. However, unlike many cities, which incorporate multiple levels of governance and a range of private utilities and property developers, campuses are governed in a more uniform and centralised way. This can accelerate the adoption of IoT devices by universities as a tool for campus management, as evidenced by the widespread adoption of 'smart campus' initiatives across the sector.

Curtin University's smart campus vision seeks to implement an IoT infrastructure to gather data on student movement and attendance to provide analytics that support a smart campus (McRae et al., 2018). These approaches connect with wider educational perspectives that champion the role of technology in enhancing student experience and learning. Analysis of this initiative found there to be potential benefits of the IoT for students with disabilities, allowing more personalised information and services. However, the benefits of these technologies were seen as being outweighed by privacy, security and interoperability concerns (McRae et al., 2018).

A University of Melbourne smart campus initiative has captured attention with its implementation of over 700 applications and IoT devices that are used to measure 'everything from temperature, energy use, room capacity and to aid in wayfinding' (Johnston, 2019). These initiatives are described in terms of 'optimising student experiences' and also making the best use of campus real estate – essentially improving the performance of the university in terms of property management and resource use.

Smart campus initiatives are an area of significant investment across the higher education sector. Many smart campus initiatives are focused on improving efficiencies in real estate management and resource use, positioning their campuses as 'living labs' to support sustainability initiatives. Aside from providing better data on student experience and management of services, smart campus data could be used as a tool for data literacy and education, supporting improved awareness of processes of data collection and also the integration of evidence and data as part of scientific policy making (Coulson et al., 2018).

2.2.5 Creative industries

IoT technologies are being used by the galleries, libraries, archives and museum (GLAM) sector to engage audiences, better understand them and enhance visitor experiences. The IoT facilitates new ways of interacting with collections and environments, supporting a variety of new approaches to curation, museum interpretation and public engagement. While these innovations are specific to the sector, they may be important tools to enhance community understanding of the IoT and to build trust, acceptance and digital literacy.

The sector could also increasingly use IoT technologies to manage the environmental conditions in which their collections and archives are stored, helping to monitor and analyse lighting, humidity and temperature control.

Case study 7: Improving visitor experience in community spaces

Smart sensors and network infrastructure were installed in three local council areas in Melbourne (Brimbank, Kingston and Port Phillip City Councils) to collect data on how public spaces (including a community library) are used and improve sustainable asset management. This includes building an interactive platform for data collection, predictive modelling of life cycle performance of assets, and to allow for live community feedback on facilities to improve service delivery and accessibility of community assets. This was funded under the Australian Government's Smart Cities and Suburbs Program.

2.2.5.1 Galleries and museums

Visitor interactions and movement data can be used to better understand how to plan, curate and design exhibitions and to understand how audiences respond to different kinds of materials and media. These relatively inexpensive approaches to IoT developments can generate new channels for interaction design and creative storytelling. They may also encourage trust of and engagement with the IoT more broadly (Coulson et al., 2018).

Australian museums and galleries are leaders in creative engagement. Audiences and technologies can be intertwined in ways that facilitate different and personalised experiences of an artwork or performance. This has been further extended through the maturation of augmented reality (AR) and virtual reality (VR). Locative media practices have explored creative ways to augment the experience of a location, often by layering historical, narrative or visual information in affective or playful ways. Relatively inexpensive technologies such as Raspberry Pi, a low-cost, small-size computer, are facilitating creative programming in ways that allow for touch and motion-based feedback, giving rise to new fields of creative media practice and audience interaction. Audio practitioners, for example, have used Raspberry Pi to program immersive sonic experiences for listeners that respond to motion and touch and can even be used to make new instruments (Abbasi et al., 2017).

In the future, the IoT may be used to support access of researchers and interested audiences to more items in a collection than can be displayed at any one time.

2.2.5.2 Libraries

The IoT could be applied in libraries to provide personalised book recommendations and alerts, including information about community events. While personalised recommendations have become the norm for streaming services, which collect data on user preferences and viewing history, this approach has not yet extended to book recommendations by libraries.

Libraries can also adopt IoT systems to better manage the experience of those using their facilities. This might include tracking room usage, temperature control, humidity levels and other environmental factors. While libraries have been using radio-frequency identification for some years, there are additional benefits to be had by integrating IoT systems into lending services. By enabling collections to be tracked and monitored remotely, the IoT can reduce the need for physical security of objects and greater accessibility by the public.

Libraries are emerging as important locations for training on digital literacy and what the IoT means for communities by providing hands-on training and workshops for diverse groups.

While the GLAM sector provides opportunities for novel IoT interactions to build trust and acceptance, it will be important that these applications are developed with suitable security and privacy measures (discussed in Chapter 3). Further research in this area would be beneficial to measure community attitudes around trust and acceptance of IoT.

2.2.6 Freight and logistics

Freight and logistics models consist of widely distributed networks; rapid information about those networks is needed for the operation of these models. IoT technologies have been embraced by this sector because they provide unprecedented real-time visibility across the entire supply chain (Lacey et al., 2015a), including real-time tracking of shipments, warehouse-capacity optimisation, predictive asset maintenance and last-mile delivery. This has led to better operational efficiency, safety and security.

In the supply side of freight and logistics, the IoT can be applied at various stages of the supply chain including warehouse, transport networks and the vehicles and crafts that are used to transport goods from suppliers to warehouses and to the customer (Lacey et al., 2015b). Efficiency, reliability, cost and capacity drive success in the supply side of the value chain, and IoT applications that can enhance these drivers and reduce cost are:

- capacity sensing: IoT systems that can detect and communicate across locations such as warehouses and ports to monitor processes in real-time and eliminate manual interferences
- planning and reporting: detecting and analysing progress within a delivery network enabling accurate delivery dates
- route optimisation: mapping the shortest or most efficient route for delivery vehicles
- safety and wellbeing: monitoring equipment and employees to increase safety and security
- resource and energy utilisation: monitoring resources and energy to enable greater sustainability and lower costs
- predictive maintenance: monitoring assets in real-time to reduce risk of failures and faults.

On the demand side, goods are transported to the customer, who expects speed and integrity of their cargo delivery, requiring security, traceability and condition reporting. IoT applications include:

- environment monitoring and management: monitoring external conditions such as temperature and condition of a parcel as part of track and trace
- threat detection and prevention: detecting unauthorised openings of parcels to reduce risk of theft
- customer experience: response times from order to delivery are tracked; integrated systems enable immediate customer feedback and satisfaction.

Future potential benefits will enable the intelligent use of an increasingly rich and complex data asset base, leading to greater efficiencies in the use of transport infrastructure, customer engagement and enhanced decision making.

2.2.6.1 End-to-end supply chain risk management

Potential threats to supply chains include natural disasters, socio-political unrest, human conflict, economic uncertainty, bio-risks, and cybersecurity. In the future, disruptions on a global scale across key trade lanes could be tracked through sophisticated IoT applications, to trigger appropriate mitigation strategies, for example, where an asset such as a warehouse is flooded, or a delivery vehicle breaks down. As systems become increasingly advanced, drawing on disparate information sources, such as weather reports and news reports, disruptions such as strikes and airport closures may be able to be predicted (McCauley et al., 2015).

2.2.6.2 Last-mile delivery

Last-mile delivery, or the final part of the delivery journey, is highly dependent on labour. As consumer demands become more sophisticated and delivery points multiply, there are new challenges for freight and logistics providers to provide cost-effective solutions for the customer, as well as internal operational efficiency. With the use of IoT and cloud-based solutions, last-mile delivery could be improved in the following areas:

- consolidation of centres and their placement
- optimising online bookings for kerbside delivery
- using vehicle routing applications
- planning after hours delivery
- defining environmental freight zone restrictions
- using distributed internet freight applications to minimise urban transport trips.

2.2.6.3 Increasingly decentralised models

Freight and logistics models will become increasingly decentralised over the next decade. It is envisaged that in the future the flow of goods will be managed autonomously by freight and logistics assets. For example, an autonomous parcel carrier will be able to save, administrate and communicate logistics process information like target destination, loading information or order priorities, and making decisions without external control. This will lead to the distribution of central control to small self-organising decentralised control units, which will act and communicate with physical objects such as switches and conveyors based on routing algorithms.

Case study 8: End-to-end supply chain monitoring

Ultimo Digital Technologies, in partnership with the University of Technology Sydney, has developed UCOT, a unique digital identification microchip system to verify that products are non-counterfeit, nor tampered with, within the supply chain. Serialised and encrypted IoT sensors are embedded into a product's package, such as a bottle, box or pallet to allow for total traceability through the supply chain. The sensor will automatically detect if a package has been opened, informing the end-user through an app. It has its own battery life, can communicate through the internet and collects information through a secure blockchain database. Data reported by the sensor includes but is not limited to: global positioning system (GPS) data to trace and map the geographical journey, temperature, humidity, exposure to sunlight and other environmental conditions.

Case study 9: Digital fish provenance and quality tracking system

Sydney Fish Market has partnered with the Foodagility Cooperative Research Centre, the University of Technology Sydney and Ultimo Digital Technologies to trial a digital fish provenance and quality tracking system, using snapper as the test species. An app will allow fishers to upload information on how, when and where fish was caught. A photo can also be uploaded to verify the species using image processing technology. Remote sensors will then track the fish on its way to the market. Information on temperature, location and smell from IoT-enabled packaging and 'eNose' technology to smell freshness, will be added to the blockchain generating a fish quality index to inform online auction trading. Data collected by this project could also be used to advise consumers about the fish that they buy.

2.2.7 Advanced manufacturing/ Industry 4.0

When the IoT is applied to the fields of manufacturing, logistics and transport, and utilities, it is referred to as the industrial Internet of Things (IIoT) (in the US) and the fourth industrial revolution or Industry 4.0 (in Europe). Both terms refer to the digitalisation of manufacturing processes, which facilitates M2M communication and intelligent, connected, self-correcting processes.

In the next five years, Industry 4.0 is likely to revolutionise manufacturing, transportation, agriculture and energy industries. IoT-enabled systems will enable the collection and analysis of data that can be used to optimise industrial processes, saving time, reducing costs and using materials with minimal human intervention.

With regards to manufacturing, Industry 4.0 has enabled the reinvigoration of a domestic manufacturing sector in Europe. For example, Adidas has established a factory in Ansbach, Germany, where IoT and supply chain consolidation have made it cost-effective to manufacture and assemble footwear, despite the high cost of maintaining a domestic workforce. The factory integrates 3D printing, automation, mass production, local sourcing of materials and IoT to respond in real-time to rapidly changing fashions and mass customisation.

Industry 4.0 offers exceptional opportunities for developed economies such as Australia, which have access to world-leading technologies in manufacturing, where automation decouples high wages from economic growth. Industry 4.0 enables flexible manufacturing processes at an affordable cost thus facilitating the manufacture of bespoke products, which is highly relevant to Australian manufacturers who generally have wide product ranges with low volumes. If Australia does not embrace the opportunities that Industry 4.0 can offer, there is a real risk that Australian companies will be locked out of global value chains as a result of their inability to comply with the processes and requirements of global original equipment manufacturers. In Europe, many original equipment manufacturers are demanding CO_2-neutral manufacturing processes, and companies such as Mercedes Benz are now making business decisions not just on the cost of a product but also on its ability to be manufactured in a CO_2-neutral way. Industry 4.0 provides a mechanism to digitally demonstrate compliance with low carbon footprint manufacturing processes, which has previously been a challenge.

2.2.8 Digital twins

While the concept of virtual models (virtual representations of a physical object or system) has existed for some time, the integration of IoT-enabled sensor networks will enable these models to be far more comprehensive in scope and scale.

Existing forms of digital modelling, such as building information modelling (BIM) software, focus on the design and construction of a building. A digital twin aims to capture a much broader array of interactions between people, infrastructure and environmental services, and to do so in real-time. It is the presence of IoT sensors, feeding and transmitting data into complex information models that allows digital twins to perform as relatively accurate replicas of their physical counterparts. Digital twins represent a step-change in infrastructure and asset management.

These models provide extremely detailed and real-time digital representations of a set of physical dynamics, components and systems in action at any given time, which can be used to capture information across the entire lifecycle of an asset or system. This enables faster modelling of an asset's lifecycle, improving diagnostics and maintenance, and the creation of new tools to optimise workplace experiences. The best-known example to date is the Singapore Government's 'Virtual Singapore' initiative.

In the future, IoT ecosystems with sensors embedded into physical infrastructure and assets may be used to create digital twins or virtual representations of properties, precincts or even whole states. Using real-time data analytics to capture complex insights, digital twins can be used to support future infrastructure planning, and improve urban resilience by supporting emergency responses to extreme weather or terrorist attacks.

However, the quality of digital twins is dependent on the quality of data integration, visualisation and analytics platforms, which will require high data volumes and diverse data streams to be visualised. Over the next decade, it is likely that the development of digital twins will be accompanied by new digital twin platforms that offer data integration and visualisation services.

Case study 10: Digital twins to support improved service delivery

A Victorian Digital Twin is being developed by Land Use Victoria and the University of Melbourne's Centre for Spatial Data Infrastructures and Land Administration. This includes using VR, AR, AI and real-time data to track and analyse scenarios in real-time, including forecasting of traffic flow predictions, power and water usage.

2.2.8.1 Digital twins in advanced manufacturing

IoT provides opportunities to create digital twins for manufacturing processes. This technology goes beyond current visualisation and engineering simulations by integrating these with real-time data analytics, augmented reality, cybersecurity systems and cloud computing software.

Sensors embedded on physical systems provide rapid and real-time information on the system they are connected to. This enables the assessment of current and future capabilities across the entire lifecycle such as:

- replicating processes of physical systems
- simulating results to discover where gaps are, to optimise an existing system
- improving future manufacturing processes
- understanding defects or problems in normal function
- refining designs and models using data simulating a system or design that has not yet been physically created (Hansen, 2020).

2.2.9 Novel data considerations

The future use of IoT devices and enabling systems will produce vast amounts of data. Preparation for this will require the understanding and adoption of 'big data' principles:

- volume: billions of devices directly and indirectly reachable; multiple levels and types of network infrastructure; significant amounts of storage, both centralised in the cloud, and decentralised within IoT devices
- velocity: high bandwidth data transfer offered by widespread fibre-optic infrastructure such as Fibre to the Premise (FTTP)/Fibre to the Home (FTTH) and wireless communication (5G/6G) (Koziol, 2018)
- veracity: accuracy, precision, trustworthiness and data provenance will be increasingly important, requiring adoption of security-by-design and risk mitigation against cybercrime.

2.2.9.1 Analytics on real-time data streams

As IoT data volumes and velocities grow, it will be necessary to apply analytics on data while it is in motion through the network, rather than trying to store the data and query it later. This improves response times and is more resilient to intermittent network connectivity. Real-time analytics on data in motion (also called distributed data stream processing) often employ the principle of moving computation and data transformation toward the data sources, rather than the more traditional approach of transferring data to computing infrastructure (O'Keeffe et al., 2018).

2.2.9.2 Data provenance

There are currently few technical mechanisms in place to enable audits of data flow and how data is used. Current practices focus on using terms and conditions of use that ask users for their consent to waive their rights to privacy and data protection.[19] As the volume of data from the IoT increases, there will be a need to audit the flow of data and its use to ensure that systems handling personal data satisfy regulatory and user requirements (Pasquier et al., 2017).

Provenance is a record of the origin of and transformations applied to data within a system. A provenance scheme to audit components handling personal data could be used to demonstrate compliance with policy and regulation and achieve accountability and transparency (Pasquier et al., 2017). For example, the European Union's General Data Protection Regulation empowers citizens, as owners of their data, to acquire intelligible records showing the source, destination and transformations applied to information about them. In Australia, the focus is on the rights and responsibilities around the use of data rather than ownership.

2.2.9.3 IoT search engines, service delivery and named-data networking

Current internet services rely on largely centralised infrastructure, such as search engines run by Google and Microsoft, to discover information. IoT data and service discovery may evolve to be significantly more decentralised, and distributed IoT search engines may emerge. There is a significant benefit to filtering data close to its source, as opposed to propagating data all over the internet (Ahlgren et al., 2012).

[19] Noting that entities defined under the *Privacy Act 1988 (Cth)* will still have obligations in the handling of personal information.

IoT resources at the 'edge' of a network,[20] where processing occurs will become sufficiently powerful and storage-rich to perform indexing and collection of data themselves without the need for direct access to cloud services. Decentralised searches will become increasingly attractive, feasible and economical. In a hybrid approach, decentralised components push some data centrally, but keep higher precision and larger data in the edge, provided that it can be kept safe. This way, some searches can be produced using traditional approaches, but decentralised queries can 'zoom in' on information that turns out to be of interest.

Distributed IoT search engine technology will lead to economic opportunities and innovation potential particularly in sensors and sensor networks, hardware and software, distributed software systems and engineering methods, and in distributed real-time data analytics and indexing. In addition, hybrid search approaches will require novel solutions for efficiency, safety and security in M2M and human-to-machine communication.

2.2.10 Ubiquitous interfaces and augmented reality

Pervasive computing focuses on building models of the environment in which technology is embedded in the context of use. Ubiquitous computing recognises that environment and the context of technology use can change, thus requiring dynamic reconfiguration (Lyytinen and Yoo, 2002). Current IoT technology can be seen as pervasive technology that is immobile and embedded into the environment. A ubiquitous IoT interface would be 'always on' while working in different environments and for different purposes, dynamically changing its appearance and behaviour.

Augmented reality (AR) is the integration of digital information into the physical world using precisely registered (visual) overlays. Extrapolating current trends in IoT and mobile and wearable technologies, products and services are likely to surface in the near future which aggregate IoT data with AR interface technology. There is significant potential for novel, geo- and context-associated content delivery, software and user-interface development, and ecosystems for user-generated AR. Also, in the foreseeable future, less obtrusive interface technologies, like glasses with visual, auditory and tactile augmentation capabilities linked to other mobile and wearable technologies, will make information access and interaction even more ubiquitous and pervasive. The IoT and pervasive AR might become the predominant form of technology-mediated perception of and interaction with our social and physical environment, in a very similar way as the internet and mobile phones have shaped the last three decades economically, socially and environmentally.

The implementation of the IoT in the technical infrastructure of smart cities and regions is likely to enable pervasive AR interfaces to develop to their full potential. Pervasive AR can allow for the more inclusive integration of people into the planning and management processes of smart cities (Clarke et al., 2019; Winter, 2019). Additionally, citizens will be able to participate in the informational enrichment of our environment, making way for Augmented Reality 2.0 (Schmalstieg et al., 2008).

[20] See definition for 'edge computing' in glossary.

2.3 IoT applications across cities/urban areas

As discussed previously, the benefit of IoT applications will span cities and regions. Smart mobility applications will be particularly beneficial in cities, in anticipation of expected population growth and urban sprawl over the next ten years. Traffic control and management alongside the deployment connected and automated vehicles (CAVs) will reduce traffic congestion and improve convenience, safety and comfort. Mobility as a Service (MaaS) is also promising, and is expected to have transformative impacts on public transport in cities.

2.3.1 Smart mobility

The IoT provides new opportunities to improve transport and mobility. Past road infrastructure investment has improved traffic congestion, reduced travel times and delays and increased road safety. However, these types of issues will become more pressing in the future as our communities become increasingly urbanised. It has been calculated that traffic congestion cost Australia $16.5 billion in 2015, and is projected to cost $27–37 billion by 2030 (Bureau of Infrastructure, Transport and Regional Economics (BITRE), 2015). Smart mobility is likely to be one of the key applications of the IoT to improve urban mobility. Through the use of the IoT and advanced algorithms, mobility solutions are likely to provide travellers with more seamless and convenient travel options across all modes of transport.[21]

[21] This includes private vehicles, public transport (buses, trains and trams), ride-sharing and car-sharing services, and on-demand micro-mobility such as rental e-bikes and e-scooters.

2.3.1.1 Traffic control and management

The application of the IoT to adaptive traffic control can allow traffic signals to adapt to traffic demand in real time. IoT devices (sensors and cameras) count cars at an intersection and the length of time they spend waiting, and the traffic controller then uses the data to optimise traffic flows. This offers benefits at a fraction of the cost of building new infrastructure, particularly when retrofitting existing roads. It has been estimated that the benefit-to-cost ratio of implementing IoT devices can be more than a dozen times greater than for building a new road (captured as traditional capacity expansion), as demonstrated in Figure 11.

More than 80 percent of vehicles sold in 2020 are likely to have devices integrated with other systems and connected via smartphones (Kumar et al., 2018). Vehicular data from connected vehicles, accessed through cloud platforms, will also enable the exchange of transport-related information (Liyanage et al., 2019) and assist in incident detection, future traffic prediction and route optimisation, which are useful for traffic control and management (Abduljabbar et al., 2019).

Case study 11: Intelligent transport systems

In 2018, VicRoads partnered with Transmax to deploy an intelligent transport system, including coordinated rate metering on a number of Melbourne's busiest motorways. Before and after studies demonstrated sustainable peak-hour flow increases exceeding 50 percent (M1 freeway), travel time reduction by 42 percent in peak periods (M80 Ring Road) and reduction in accidents by 60 percent (CityLink tunnel). Economic benefits were estimated at $2 million per day, including reduced fuel and consumption costs. It was also estimated that greenhouse gas emissions were reduced by 11 percent (Transmax, 2018).

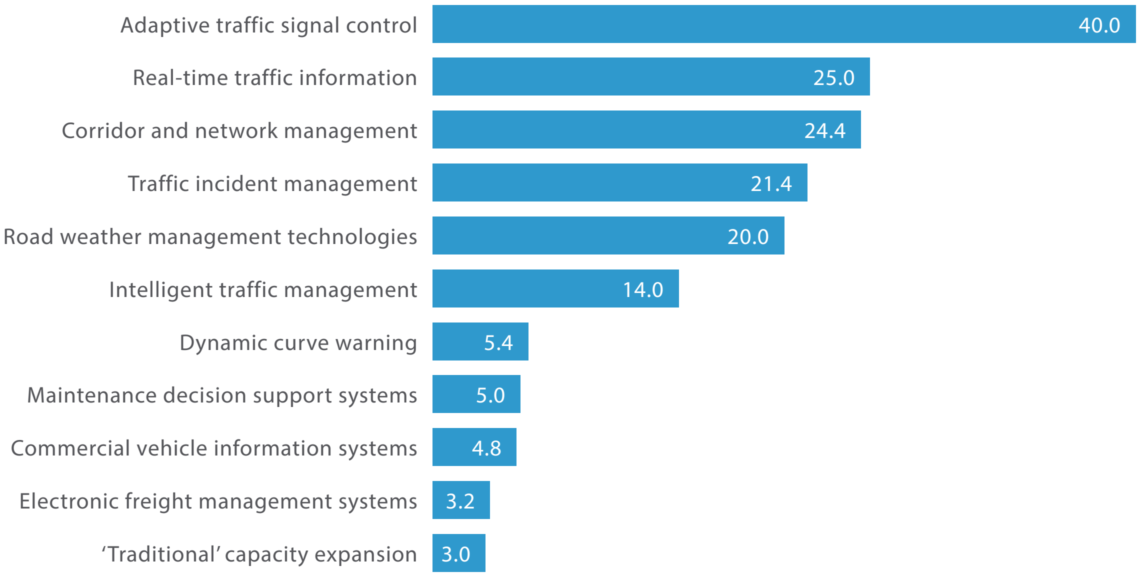


Figure 11: Average benefit-cost ratios of transport investments

Note: Values vary depending on many factors, including base conditions used for comparison.
Adapted from Dia, 2017.

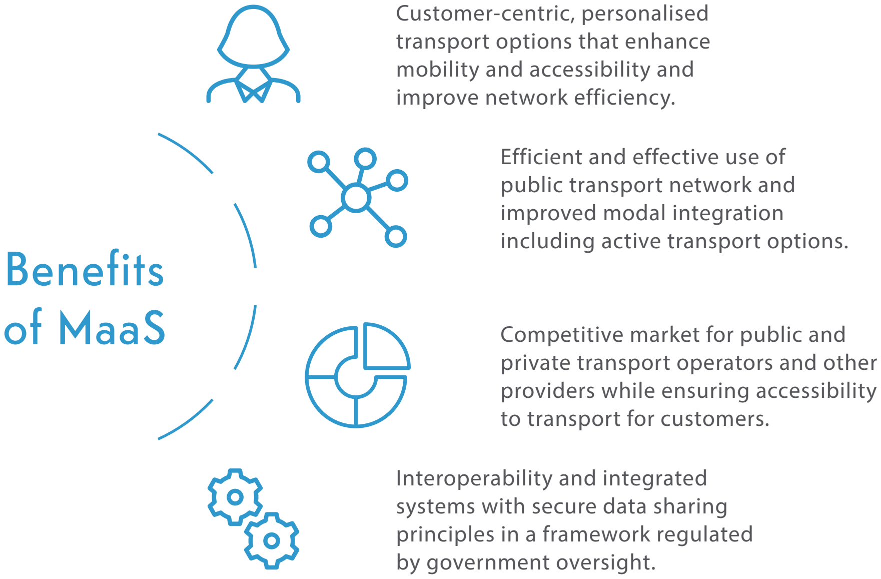
2.3.1.2 Mobility as a Service

MaaS systems are a developing concept that use a single portal to allow users to plan a journey based on their personal preferences. These preferences can include cost of the journey, length of travel time and method of transportation (e.g. train, taxi, bikeshare, carshare). Currently, MaaS applications are provided by smartphone apps or other mobile technologies. While similar journey-planning concepts to MaaS exist, such as Google Maps, a key feature of a MaaS system is its streamlined approach to planning, booking, electronic ticketing and payments across all modes of transportation (public or private) through a single portal using a single charge. Future development of MaaS with other technologies, such as AI and automated decision making, has the potential to improve customer choices, reduce travel costs, and increase network capacity and transport sustainability, improving social and environmental outcomes (Intelligent Transport Systems Australia, 2018).

Case study 12: Mobility as a Service app

SkedGo has partnered with iMOVE Cooperative Research Centre (CRC), IAG and the University of Sydney to trial a MaaS app to provide multi-modal transport options with real-time updates to volunteers. Using a customised version of SkedGo's TripGo, eligible participants in the Greater Sydney area will be able to find, compare and book multi-modal transport bundles through this app via subscription plans. Transport options include public transport (such as train, tram, ferry and bus), as well as a large portfolio of car-based transport services (e.g. taxi, car rental, Uber, Car Next Door and GoGet). Passengers will be able to find, compare trip options (in terms of cost, travel time, emissions and health benefits), book trips and pay through the app.

This service will use Sydney's open data platform to aggregate open and private data sources to provide insights and understanding of travel behaviour as well as infrastructure utilisation by trial participants.



Benefits of MaaS

Customer-centric, personalised transport options that enhance mobility and accessibility and improve network efficiency.

Efficient and effective use of public transport network and improved modal integration including active transport options.

Competitive market for public and private transport operators and other providers while ensuring accessibility to transport for customers.

Interoperability and integrated systems with secure data sharing principles in a framework regulated by government oversight.

Figure 12: Benefits of MaaS

Adapted from Intelligent Transport Systems Australia, 2018.

Challenges to the widespread uptake of MaaS include government buy-in, open public–private partnerships, the inclusion of municipal transportation (buses and trains) size optimisation, passenger demand prediction, and providing reliable and timely services to users. Overcoming these challenges will provide opportunities to enhance performance from commercial, operational and user-acceptance perspectives. Emerging IoT applications that increase access to real-time data are likely to help with optimising these future on-demand services.

2.3.1.3 Connected and automated vehicles

CAVs represent a potentially rich environment for the development and deployment of IoT and cloud-based services; they are expected to have wide impacts (Fagnant and Kockelman, 2015). The hardware architecture in CAVs is comprised of actuators, sensors and a computer system, while the software component comprises the AI self-driving system, navigation modules, localisation algorithms and perception systems to detect moving objects (Chong et al., 2012).

The IoT is expected to play an important role in road safety and in minimising road crashes and injuries. On-board IoT devices can be used to monitor vehicle conditions, the environment, the driver and speed, detect incidents, and provide warnings to inform drivers and road agencies of any hazardous situations. The National Transport Commission is working with the Australian Government and state and territory governments to develop regulatory reform options to support the safe, commercial deployment of automated vehicles (National Transport Commission, 2019).

As part of this, vehicular communication in CAVs (V2X, that is vehicle communication to anything) will play an important role in the next generation of these intelligent transport systems.[22] Recent research showed the benefits of V2X to include: increased pedestrian safety (Xu et al., 2019), reduced vehicle crashes through advanced warning systems (Khan et al., 2019), improved network capacity, stabilised traffic flow and reduced emissions by using cooperative adaptive cruise control systems (Milanés et al., 2014).

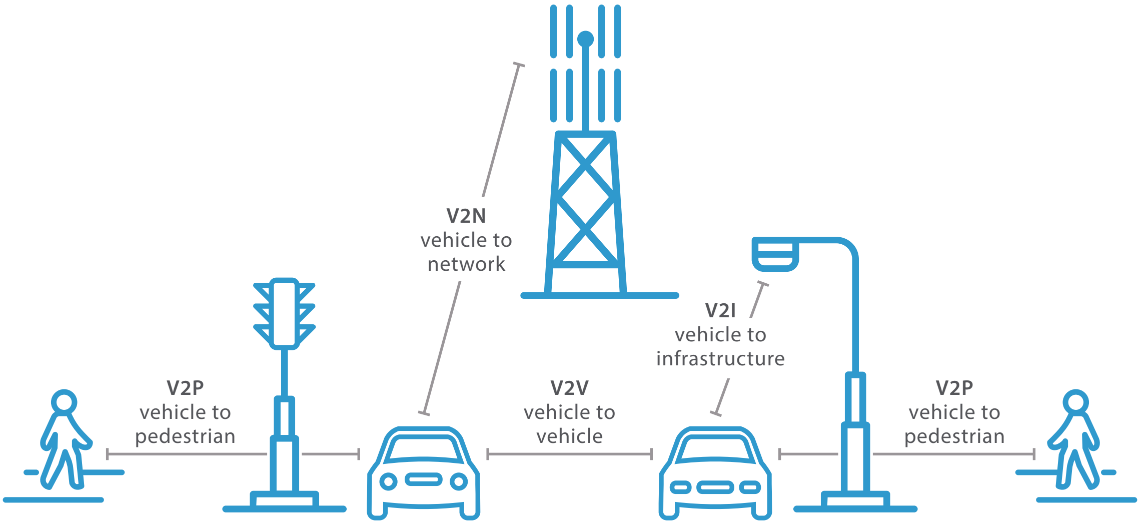


Figure 13: V2X communications can enable smart mobility and automation in cars

Adapted from McKinsey & Company, 2019.

[22] This includes vehicle-to-vehicle (V2V), vehicle-to-roadside (V2R), vehicle-to-barrier (V2B) and vehicle-to infrastructure (V2I) messaging.

2.4 IoT applications in rural, regional and remote areas

IoT applications that will provide benefits specifically to rural, regional and remote (RRR) areas are centred around responsible resource management and promoting ecological sustainability, including prevention and management of environmental disasters such as bushfires. Improving road infrastructure and road safety is also a key application. These applications are discussed in more detail below.

2.4.1 Sustainability and resource management

In RRR areas, connected sensor networks can be used to improve existing sustainability and resource management practices, providing data insights to refine and update existing practice, while reducing wastage and lowering costs. This can be applied in areas such as mining, precision agriculture, ecological sustainability, and smart water management to increase operational efficiency, increase worker safety, conserve resources and manage resource use. For example, IoT has high utility in agricultural management including: integration of sensors into agricultural machinery to guide inputs and operations, providing precise information on soil and water conditions, reducing stock handling by monitoring animal health, and improving visibility in supply chains around provenance, sustainability and ethical considerations to inform customer purchasing decisions (Rural Industries Research & Development Corporation, 2016).[23]

Case study 13: On-farm monitoring

The IoT company NNNCo started to roll out a 3 million-hectare IoT network for cotton farmers in 2019. The network will provide data on soil moisture through the use of sensors, including soil probes, rain gauges, local weather data, water and fuel tank monitors, and satellite imagery. This will enable better scheduling of irrigation and subsequently a reduction in water use.

Case study 14: Monitoring impacts of urban glow

The Bundaberg Regional Council's Reducing Urban Glow project trialled the use of urban glow sensors to measure light pollution and its impacts during the marine turtle nesting season. A publicly accessible web-based heat map was also developed to raise public awareness and support engagement for place-specific interventions to reduce urban glow. This was funded under the Smart Cities and Suburbs Program.

2.4.2 Prevention and management of environmental disasters

Australia has historically been subject to extreme weather conditions. While it is difficult to attribute a single weather event to climate change, research forecasts that climate change will increase the frequency of hot and dry winds from the centre of the continent and the extent of drought (CSIRO, 2020). Traditional prevention methods for disaster management, such as pre-emptive hazard reduction or back-burning for bushfires, should be supplemented by modern solutions, such as IoT technologies, to assist in modelling risks and vulnerabilities to improve Australia's prevention of and response to extreme weather events (Biggs et al., 2016).

[23] Further information on IoT applications in agriculture can be found in the ACOLA Report *The Future of Agricultural Technologies* (Lockie et al., 2020).

With the help of IoT sensors and AI-driven analytics, real-time and accurate data can be collected to improve decision making prior to, during and after a natural disaster occurs. Sensors and unmanned drones can provide weather data, satellite images and archived data, which can be combined with modelling tools to map complex topography for modelling the risk of wildfire (Biggs et al., 2016). Data acquired from IoT networks that track human and animal population mobility could inform prevention strategies such as informing back-burning strategies or ensuring that pathways for escape are clear. By gathering diverse ranges of data for analysis and modelling, predictions can be made about the likelihood of an event occurring, and its predicted impacts, with more speed and accuracy which can improve disaster planning (Tuffley, 2019).

These data can be passed to emergency services and local authorities to improve situational awareness for better disaster management and response. To facilitate this, state emergency service departments could consider integrating emerging IoT technologies with their existing systems so that accurate and targeted information can be strategically deployed directly to the correct local authorities (Tuffley, 2019). Connectivity will be an important enabler for the success of these systems and is discussed in more detail in section 4.5.3.

Case study 15: Environmental monitoring

Following events such as the Black Saturday bushfires and Hazelwood Mine fire, Victoria's Latrobe Valley has installed a sensing network that enables 24-hour monitoring to measure air quality, micro-weather, soil moisture content and 360-degree thermal and visual imaging. All information is loaded on the Latrobe Information Network website, allowing residents to monitor conditions in the area. The network includes bushfire ignition detection and flood level monitoring, and sending alerts with thermal and visual images to emergency services if an incident is detected.

Case study 16: Satellite technology for bushfire prevention and response

The SmartSat CRC is exploring emerging satellite technology for bushfire prevention and response. The use of low earth orbit (LEO) satellites could provide connectivity to mobile phones in RRR areas in the event of anticipated or actual damage to mobile cell towers (Shepherd, 2020). Satellite technology could also enable cameras on mobile cell towers or drones to be used for smoke detection so that incidents can be immediately reported to emergency response centres.

Similar technologies are being developed in Spain (Universidad Carlos III de Madrid, 2019) and the US. The Los Angeles Fire Department has been using firefighting drones since 2017, locating hot spots with infra-red cameras, dropping water or retardant, and guiding firefighters out of danger. However, it will be important that operators are given sufficient training, as drone effectiveness is highly dependent on operators' skills (Shieber, 2019).

Case study 17: Monitoring biodiversity recovery post environmental disasters

In the wake of environmental disasters such as floods, fires or cyclones, the monitoring of wildlife recovery is important. CSIRO, in collaboration with scientists from Brazil and Spain, have developed a distributed, wireless sensor network with autonomous nodes that continuously monitor diminishing biodiversity in the Amazon jungle. This system could be applied in Australia to monitor the recovery of wildlife, including endangered species, following environmental disasters (CSIRO, 2017).

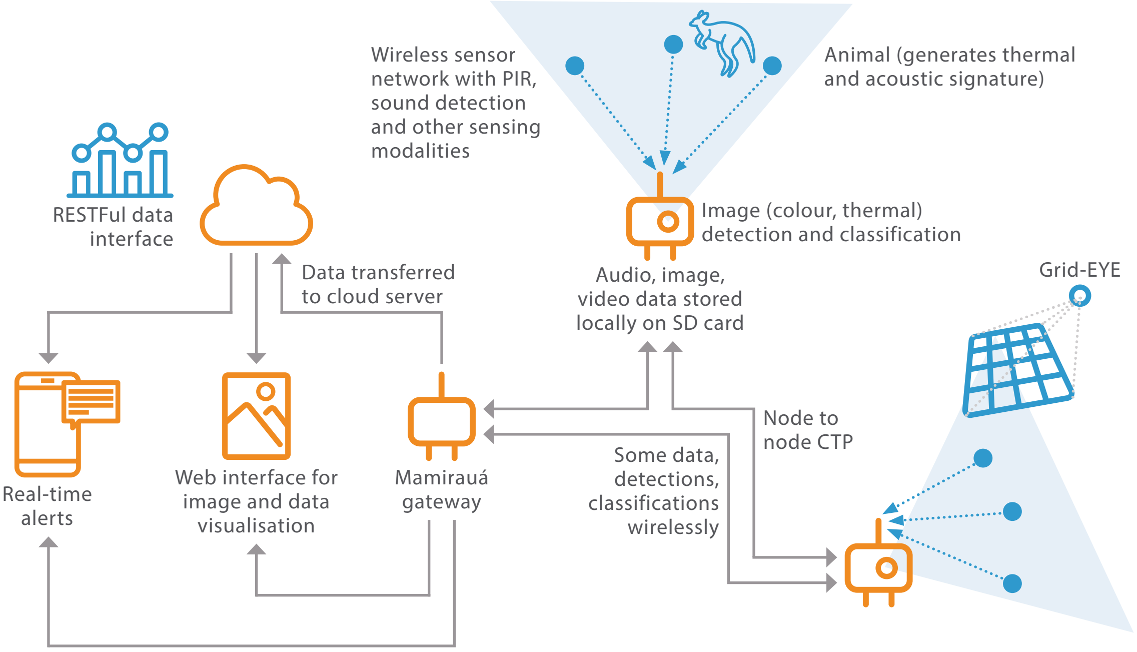

Wireless sensor network with PIR, sound detection and other sensing modalities
Animal (generates thermal and acoustic signature)
RESTFul data interface
Image (colour, thermal) detection and classification
Data transferred to cloud server
Audio, image, video data stored locally on SD card
Grid-EYE
Node to node CTP
Some data, detections, classifications wirelessly
Real-time alerts
Web interface for image and data visualisation
Mamirauá gateway

Figure 14: Overview of planned network architecture to monitor biodiversity

Adapted from CSIRO, 2017.

2.4.3 Smart road safety

IoT applications in mobility are similarly applicable in RRR areas as urban areas, especially in terms of safety. However, long distances and limited resourcing makes IoT road safety applications in RRR areas particularly valuable. For example, rural road crashes contribute substantially to the overall road toll in Australia (Dolman, 2019). Incident-detection through the use of on-board vehicle systems in CAVs could provide real-time information about on-road hazards to drivers, as well enable emergency services to respond to incidents quickly and more accurately with geo-location data. However, cellular coverage and connectivity are likely to be the critical barriers for deployment and could impact on the ability of CAVs to operate on all rural and remote roads (WSP, 2018).

Case study 18: Smart road barriers

Smart road barriers were trialled in South Australia on Victor Harbour Road in 2013. The wire rope technology sends an electronic message direct to the city's traffic management centre when a vehicle crashes into the barrier, immediately alerting police and ambulance crews. This has resulted in a reported 80 percent reduction in cross centre line casualty crashes. The tension of the wires can also be monitored and any impact or loosening is reported to a management centre allowing a work crew to be dispatched (Dua and Anderson, 2013).

2.5 Key opportunities and challenges

This section outlines some of the key opportunities and challenges to support the responsible and considered deployment of IoT. Broad considerations to support policy development to maximise opportunities and mitigate risks in smart cities and regions are raised including the importance of evaluation of existing measures as well as assessment of economic opportunities from the data that will be captured from the IoT in the future. Challenges include interoperability and vendor lock-in, the importance of data usage and integration by governments, privacy and security challenges, and the importance of strengthening telecommunications resilience. This is followed by discussion on a number of sectors which represent key opportunities for IoT applications in Australia.

2.5.1 Evaluation and investment opportunities

The Australian Government's Smart Cities and Suburbs Program has accelerated investment in IoT technology by local governments across urban, regional and rural areas. Ongoing and future investment should be considered in the context of specific challenges facing a particular community, in order to avoid a deployment that has limited scalable impact. Many of the programs funded through this initiative have been rolled out over a 1–2 year period, with relatively limited opportunity for scaling or integration into business processes.

As the number of projects and use cases of IoT increase, providing a forum for governments and other stakeholders to collaboratively compare and evaluate the successes and challenges experienced will be critical. There needs to be a consistent focus on learning from these short-term trials and pilots to determine the best solutions. This will increase the overall utility of these initiatives, reducing waste, cost and efforts nationally. A recent study on smart cities would be useful for governments to consider in this process. Yigitcanlar et al (2020) evaluated 180 local government areas (LGAs) in Australia against a number of smart city performance indicators: productivity and innovation, liveability and wellbeing, sustainability and accessibility, and governance and planning. The study suggested that all LGAs were relatively strong in the liveability and wellbeing category (particularly in safety and security and housing). General areas of weakness were in sustainability and accessibility (sustainable buildings, vehicles and energy) and governance and planning (public connectivity options and smart city policy). The report highlighted that there were major regional disparities with metropolitan LGAs gaining higher performance outcomes. The report recommended ongoing investment and support mechanisms by state and territory government and the Australia government to deliver impact in rural and regional LGAs.

The report recommended taking an integrated approach on the following pillars to achieve success for smart city projects:

- **focusing on developing technology unique to the challenges and needs of each LGA**, which will help contribute to prosperity and a local innovation economy
- **ensuring that technologies are inclusive** (i.e. appropriate, affordable and effective)
- **adopting sustainable urban development principles** to address the global climate crisis (addressing issues such as urban footprint, emissions, urban waste and food security)

- **equipping cities with highly dynamic mechanisms** to plan urban growth and manage day-to-day operational challenges
- **taking a holistic and balanced approach** regarding the above factors.

While these principles apply to the development of smart cities generally, they will also be consistent with decision making and evaluation of IoT initiatives. As the report cautions, technological solutions will not always create positive outcomes, and consideration of the above points will ensure that technological innovations such as the IoT strengthen, rather than 'weaken social compacts as to prevent fractures that result in fragility of cities' (Yigitcanlar et al., 2020, p. 16). A broader consideration of these factors from a holistic ecological lens would be beneficial over the next 5–10 years (section 4.6.5).

2.5.2 Economic opportunities from cities and regions data

The adoption of IoT in industry has mainly been understood as a technology that can be used to optimise systems and processes through centralised data system to increase productivity and reduce costs. This is particularly relevant for asset-heavy sectors such as mining, manufacturing, construction and logistics. However, the IoT should also be considered as a disruptive technology – the data acquired from IoT is a rich, new source of economic value, and automated decision making may fundamentally change our current economic structures and organisations. For example, the use of IoT in households may present new capabilities and create new sources of income (for example, where, in the future, excess solar energy may be able to be sold back to the national grid through distributed energy resources), or create new opportunities in law (where smart devices are used to confirm provenance and quality of products in smart contracts) and in insurance (where more personalised insurance premiums are offered through new volumes and granularity of available data).

It will be important for Australian governments and businesses to begin to consider the structural economic disruption that the IoT is likely to bring, rather than just economic benefits in terms of productivity growth or cost-efficiencies in sectors. This will include considering the relationship between the IoT and other parts of the emerging digital technology stack, which includes blockchain, distributed ledger technologies and machine learning.

Questions of data ownership and the implications for decentralisation will also be fundamental to understanding and forecasting the economic disruption and changes that the IoT is likely to create. Any further economic analysis of IoT adoption and innovation should focus on the microeconomic aspects of information economics, transaction cost economics and industrial organisation, rather than macroeconomic models that focus on expenditure.

2.5.3 Interoperability and vendor lock-in

Challenges for service delivery though the IoT include a lack of interoperability and cross-sectoral integration of smart data. A key stakeholder to this report, Dr Sarah Barns, noted that NNNCo, a technology vendor working across smart city projects in Australia has described the issue in the following way: 'During the past 24 months we have regularly encountered customers who have a device, the means for transmission and a platform, but the protocols and their platform will not talk to each other.' Such issues will hinder the transformative potential of the IoT, particularly as governments move towards greater integration of IoT applications for service delivery. The issue of interoperability is discussed in more detail at section 4.6.2.

2.5.3.1 Vendor lock-in

A related issue to the interoperability challenge is the issue of vendor lock in. Where customers have been dependent on a single technology provider, this may restrict the ability to transport data and application services to a different vendor without substantial costs, legal and regulatory constraints, privacy and security implications and technological incompatibilities. Individuals and organisations may often not understand the complexity and cost of switching or porting from one vendor to another until after a contractual agreement has been entered into. This can restrict access to better pricing, choice and innovation (Opara-Martins et al., 2016). In IoT deployment, examples of vendor lock-in include point-solution technologies, such as smart parking or smart lighting, which don't scale or connect with other services (Barns, 2019b; B. Cohen, 2015; Internet of Things Alliance Australia, 2017c; R. Robinson, 2016). While this issue is not specific to the IoT, it is of high importance, as the maturation of the IoT and cloud computing sector is likely to exacerbate the risk of vendor lock-in. Vendor lock-in was raised as a particular concern in stakeholder consultation for this report.

However, there are positive developments to mitigate the risk of vendor lock-in. For example, middleware companies like NNNCo and Meshed Network, are beginning to position themselves as suppliers to support local governments with data harmonisation and normalisation in the deployment of smart city solutions. International standards development and industry cooperation is also likely to support a competitive environment that promotes portability and interoperability.

In Australia, the use of principles-based standards will limit the risk of vendor lock-in by ensuring that certain vendors or a specific technology are not given an unfavourable advantage over others in the market, and to enable a competitive market sector. This is discussed further in section 4.2. Participation in international standard-development forums is also important to ensure that national interests are represented and to support the growth of domestic industry players offering potential middleware solutions.

Case study 19: International developments to prevent vendor lock-in

Growing concerns by European organisations about data sovereignty and security, given increasing reliance on market-leading, largely US-based cloud providers, have led to the emergence of the GAIA-X project. This project, established in 2020, will create an efficient, secure, distributed and sovereign European data infrastructure for industry and users, with support by Germany and France, and collaboration between major companies, including Bosch, SAP and Festo. Rather than establishing itself as the next global cloud provider, GAIA-X aims to enable the participation of many specialised providers across Europe in a distributed and interconnected data infrastructure. It will also support decentralised processing (edge, fog, cloud) and multi-cloud strategies, reducing the risk of vendor lock-in. Multi-stakeholder governance for trustworthy and certified services will ensure that EU standards are upheld (Weiss, 2019).

Post-supply restrictions on consumers

Another critical consideration around vendor-lock relates to the restrictions that may be placed on consumers following sale or supply of an IoT device. While the initial purchase might be straightforward, post-supply obligations can severely restrict a customer's choice for third-party service providers or the subsequent purchase of other products. As a result, competition may be hampered. For example, customers may be required to enter into an ongoing service contract (e.g. for cloud data processing and storage) which provides an additional revenue stream. All IoT devices contain some form of software and, in the future, could also contain a substantial amount of digital content aside from software. Therefore, intellectual property constraints may also be leveraged by the provider to protect potential revenue streams.

Consumers may be unaware of such obligations at the time of purchase. Other obligations may include posing restrictions on use and resale (where software essential to the functionality of the device is non-transferable) and penalties for breach of use restrictions. For example, if customers wish to make their own repairs to an IoT device, such as a connected vehicle, they may need to access integrated software and face both legal and technical barriers or be penalised for breaching end user licence agreements or copyright legislation. Or, if a user would like to buy a different brand of the same product but is unable to transfer historical data from their original device.

Providers might use their remote disablement capacity to lock down software for a perceived breach of copyright law or contractual conditions. A connected IoT device could also be remotely disabled if a purchase instalment or a related service fee has not been paid.

Other forms of disablement are less direct and much less likely to be subject to overt customer agreement or understanding. For example, a provider may issue an upgrade to firmware or software that reduces the speed of the IoT device's data-handling capabilities to a level that makes the hardware unusable. A service provider may go into liquidation or decide to discontinue a service, such as cloud data storage and processing. This can make an IoT device useless if it was designed to communicate only with a proprietary service. A customer may have no choice but to buy a new device with upgraded hardware or to pay a premium price for an upgraded service. Other than the impact on individual customers, this will also increase the IoT's contribution to increasing the amount of global e-waste.

Digital content that resides in, or is accessed through, IoT devices may also be blocked to protect rights holders. This may be legitimate when there is no record of a user holding a licence to that content but could also happen even if a customer has not been involved in a breach of contract or any wrongdoing. While the IoT device might have been fit for purpose as originally supplied to the user, it may be only afterwards, by a deliberate or inadvertent act by the supplier (or someone else in the provider network), that this changes. A provider's ability to act in this way is often supported by non-negotiable contractual terms explicitly granting the right to such modifications.

For several years, US farmers have been disputing the attempts of Deere & Company (John Deere) and other manufacturers to restrict their rights to repair their internet-connected agricultural machinery, which contains closed-source embedded software and technological protection mechanisms (TPMs).[24] Currently there are negotiations by industry associations to provide farmers' access to software provided to authorised dealers by 2021, and other states are also looking at legislative measures (Waldman and Mulvany, 2020).

In response to some of these issues, the ACCC launched an inquiry in 2020 into after-sales markets for agricultural machinery examining access to third-party repairs, as well as privacy and competition concerns around data ownership and management (Australian Competition and Consumer Commission, 2020).

2.5.4 Usage and integration of data

Australia faces particular complexities regarding data governance, as many major cities lack a single government 'champion' capable of implementing city-wide data initiatives. There is an opportunity for a more integrated or interoperable approach to data and device management. For example, if activity data generated by smart lighting services were published in a standardised format, they could be used in different applications or integrated with other datasets to provide richer data analytics.

The incorporation of data from the IoT also provides an opportunity for the Australian Government to co-ordinate the delivery of improved data assets to inform decision making across the three levels of government, building on existing work by governments. This would enable better sharing of government data to form improved data assets, which could include data drawn from different levels of government, industry and academia.

For example, in 2017, the Australian Government introduced a National Cities Performance Framework to better monitor the relative performance of Australia's urban areas. Data are collected across a range of standardised indicators and published in a common dashboard online. The dashboard uses two kinds of indicators: those that measure progress of cities across key indicators and those that provide contextual information about a city and why it performs the way it does. These initiatives provide opportunities for experimentation in the use of IoT data to support dynamic monitoring of urban settings. Over the next decade, data accessed via the IoT could also be used to improve the monitoring of cities and regions' performance against international obligations and indicators, such as the United Nations 2030 Sustainable Development Goals. Although IoT initiatives are carried out at state and local levels, it would be practical for the Australian Government to provide national oversight, as international targets and obligations are determined at a national level.

The process of data integration needs to include more connected decision making processes, drawing from broader sources of data and intelligence. Building on the benefits of digital services and data to improve the way a city works cannot be realised by investing in distributed sensors and technology solutions alone. Such shifts necessitate a 'reinvention of governance', which involves 'transforming the way they work internally and together with outside partners and citizens' (Arup and London, 2014, p. 32). It is worth noting that cross-jurisdictional collaboration is particularly important for Australian cities where the three levels of government overlap (Barns et al., 2017), as local governments may not have access to infrastructure assets owned by a different level of government.

[24] TPMs are software, components and other devices that copyright owners use to protect copyrighted material from infringement. Examples include encryption of software, passwords and access codes.

2.5.5 Privacy and security

2.5.5.1 Mitigating vulnerabilities to critical infrastructure

A key challenge for IoT service delivery applications in smart cities and regions is the issue of vulnerability. As more and more connected devices are introduced to everyday environments and critical infrastructure (e.g. telecommunications, energy grid, and emergency communications), more surfaces are available to the risk of remote interference and hacking. Most IoT devices currently have limited computational capabilities to run sophisticated encryption and authentication algorithms for secure communications systems. This could expose national infrastructure to the risk of large-scale and systemic failures if breached by physical and virtual attacks. For example, an attack on the national energy grid could jeopardise the network and lead to a system-wide blackout. Recovery may have significant costs, impact economic productivity and lead to loss of confidence by the public. This issue should be considered further – for example, by utilising the decentralised and distributed nature of IoT networks, much like the conventional internet, to mitigate vulnerabilities, such as using edge computing, networked microgrids and blockchain technologies to make systems secure and efficient in a scalable manner (Li et al., 2018).

Other steps to mitigate these risks include backing up data systems, ensuring software and security systems are robust and up to date, and purchasing cyberinsurance for national and state systems.

2.5.5.2 Platform business models and security and data challenges

Existing commercial platforms are seeking to extend their ecosystems into IoT environments through smart home devices and smart city initiatives. Other service providers are also seeking to use the IoT to generate and commercialise data assets. Existing business models on data use are leading to challenging obstacles in interoperability. While interoperability and data sharing are both ideals underpinning the IoT, these also come with security and privacy challenges. In this respect, it is also important that Digital Platforms Inquiry recommendations be considered in relation to the future impact of platform business models on the dynamics of the IoT.

To address vendor lock-in and the concerns regarding urban governance, data privacy and data surveillance, governments could consider the implementation of APIs, city data marketplaces and open data collaboratives or 'trusts' that seek to create common protocols and frameworks for data sharing across vendors, public–private agencies and citizens.[25] This could align with current work on the Data Availability and Transparency Bill, the Australian Privacy Principles (APPs) and *Privacy Act 1988 (Cth)* (the Privacy Act), as well as state and territory frameworks for sharing government data, including privacy laws and freedom of information requests.

For example, Copenhagen has a city data marketplace where third party data can be used to augment public sector data and where data can be bought or sold.

[25] Examples include the Copenhagen Data Marketplace, the European DECODE Project underway in Amsterdam and Barcelona and the X-Road initiative implemented in Finland and Estonia(Raetzsch et al., 2019).

Case study 20: Open data hub

In 2016, Transport for NSW established the Open Data Hub, which gave open access to transport data through static datasets and real-time APIs. This enabled customers, developers and analysts to use data to create innovative transport apps, as well as insights and information services for customers. Since its launch, over 2.2 billion API hits have been counted on their Open Data Server. Benefits listed by Transport NSW include:

- promoting open, transparent and accountable government
- contributing to the digital economy in NSW and promoting the development of new businesses and industries that can make use of government data
- leading to better public services
- advancing community engagement with the government and with the work of government
- enabling data sharing between government agencies in NSW and across jurisdictions
- facilitating greater understanding of agencies' own data and the potential of that data
- supporting evidence-based policy making and policy research.

For example, My House Geek has used these data to develop an interactive map which allows users to explore a neighbourhood through a digital map before moving. A user can search for properties, as well as discover nearby schools and public transport services.

Data are democratised and this allows community members and industry to generate insights and contribute to the digital economy to support new businesses that can use these data. The Copenhagen City Data Exchange 'has enabled public and private sector organisations to gain insights into data use cases, new external data sources, GDPR issues and to explore the value of their data' (Wray, 2018). Governments could also consider controlled access data sharing arrangements with companies to facilitate information exchange.

Leadership by Australian governments in these types of initiatives would support openness, transparency and accountability in the characteristics, management and release of these data, and improve community trust and acceptance of data usage and management.

2.5.6 Growing politicisation of service delivery

Major technology companies are likely to use advances in the IoT to extend the reach of their existing platforms into urban domains (Barns, 2019b; McNeill, 2015; Sadowski and Bendor, 2018). This has already led to a growing politicisation of urban governance, data privacy and data surveillance concerns (Barns, 2019b; van der Graaf and Ballon, 2019). For example, Google's sister company Sidewalk Labs has sought to enter the urban innovation space by seeking to build a city 'from the internet up' using IoT and other smart city technologies. This has attracted widespread criticism from residents, concerned about the capacity for Google to use this initiative to advance its data commercialisation and AI, or deep learning, strategies (Lorinc, 2018). Governments will need to continue to assess their ongoing engagement with major technology companies that provide IoT solutions, as public versus private interests converge, particularly in the ownership, use and security of data.

2.5.7 Strengthening telecommunications resilience

An increased uptake of IoT systems over the next decade across cities and regions and in different industry contexts will be dependent on reliable connectivity. Multi-modal connectivity solutions which include redundancies will ensure that IoT systems remain online and functioning. In particular, the recent 2019–20 bushfire season demonstrated our dependence on reliable connectivity, which will be critical for future bushfire prevention and response, particularly emergency management.

In the event of bushfires, for example, damage to telecommunications infrastructure or power outages could increase the risk of service outages. As a result of the 2019–20 bushfires, the ACMA reported that 1,390 facilities were either directly impacted by fire damage or indirectly impacted by power outages or other factors. Fifty-one percent experienced outages of four hours or more during the review period. Most outage incidents were a result of power outages, rather than direct fire damage (which only accounted for one percent of outage incidents), indicating that mains power affected network resiliency (Australian Communications and Media Authority, 2020b).

The Australian Government is investing $37.1 million to strengthen telecommunications resilience in bushfire and disaster prone areas so that communities can stay connected during emergencies. Initiatives include improving the resilience of regional and remote mobile phone base stations to upgrade longer-lasting backup power sources, delivering improved communications over the next two bushfire seasons and deploying satellite services to provide additional redundancies to improve telecommunications for rural fire authorities and evacuation services (Minister for Communications, Cyber Safety and the Arts, 2020).

Other back-up options that could be explored include maintaining legacy copper-wire networks, using high-altitude balloons to create aerial wireless networks (Critical Comms, 2019) or deploying satellite technologies (see Appendix B). The use of mesh networks has also been raised as a possible resilience measure, where people in a disaster-afflicted area could use a 5G-enabled smartphone as a node to connect to other phones (Tuffley, 2019). Further research on distance ranges and population density will be critical as emerging technologies evolve, to understand the applicability of these technologies in more remote areas.

2.5.8 Advanced manufacturing

Workforce training is critical for ensuring that Australian industry is ready for the Industry 4.0 revolution. In 2019, the World Manufacturing Forum published a report outlining not only the skills the workforce will need to develop but also a number of emerging roles (World Manufacturing Foundation, 2019). These included detailed descriptions of the responsibilities for a number of emerging roles, including digital ethics officer, a lean 4.0 engineer, an industrial big data scientist, a collaborative robotics expert, an Information Technology/Operation technology integration manager and a digital mentor.

Another recent report identified that Australia has both a productivity and an innovation gap (Innovation and Science Australia, 2017). The report highlighted the opportunity to bridge the productivity gap, a measure of the efficiency of labour and capital, through the application of advanced automation and digitalisation. Amongst OECD nations on the Global Innovation Index, Australia is ranked 10 on innovation inputs; however, it is ranked 72 on research business collaboration (Innovation and Science Australia, 2017). Industry 4.0 offers an opportunity to assist in bridging these gaps, which will give Australia the opportunity be a leader in the global innovation race which is valued at $1.6 trillion (Innovation and Science Australia, 2017).

As previously noted, there are also particular opportunities for Australia to develop digital twin technology over the next decade, given our highly educated workforce and sophisticated economy. While this technology is relatively new, the value is likely to rise exponentially over the next decade and eventually overtake the value of the manufacturing process equipment.

A challenge for advanced manufacturing is the development of wireless communications with high standards of reliability, latency and security (i.e. ultra-reliable low-latency communications, URLLC). Despite the academic research and on-going standardisation efforts towards URLLC (which will include 5G and WiFi 6), there remain many challenges, including how to ensure ultra-high reliability and low latency within the limited radio spectrum.

2.5.9 Energy management

The IoT is likely to encourage new business models in energy management, which bundle electricity with other services or facilitate peer-to-peer energy trading (Australian Energy Market Operator (AEMO), 2020).[26] While opportunities for peer-to-peer trading are currently limited and complex for Australian households, recent research has found a strong interest in energy-sharing platform models (Strengers et al., 2019). There are indications that a variety of options for bundling, sharing and trading energy will emerge both locally and internationally. Broader energy considerations are discussed in more detail at section 4.4.1 and 4.6.6.

Case study 21: Intelligent energy management

Evergen, an Australian energy software company, uses an intelligent energy management system developed by CSIRO to help customers manage and monitor their solar panel and battery systems. The system autonomously checks weather forecasts and telemetry from panels and grid conditions, to optimise usage and allow battery charging at off-peak times. Evergen's 'virtual power plant' system allows customers to sell energy into the wholesale market and pay to charge batteries when prices are negative. The cost of installation of solar photovoltaic systems has typically been a barrier to uptake and adoption, but Evergen has forecast that its system will reduce the return on investment from 8–10 years to 5–6 years (Fowler, 2019).

2.5.10 Health delivery

2.5.10.1 Redefining healthcare systems post-COVID-19

While the challenges that COVID-19 has presented are likely to have lasting social impacts, it has also afforded new opportunities to challenge and redefine traditional concepts of primary, secondary and tertiary healthcare. The use of IoT and other digital technologies in this crisis are already showing positive impact. They have augmented and enhanced traditional clinical settings through the use of population health monitoring, medical wearable devices and enhanced telehealth initiatives to improve remote monitoring. This has reduced patient load on the healthcare system and reduced the risk of transmission. Current use cases have demonstrated the interconnectedness between IoT, AI, deep learning and blockchain, and the importance of considering these technologies and their impacts collectively.

[26] See Case study 2: Innovation in water management practices.

It is likely that these applications will increase public and government acceptance of such technologies, which may impact on other areas of future healthcare (Ting et al., 2020). For example, while the focus of healthcare systems and governments has been to tackle the direct impact of COVID-19, it would be beneficial to assess the long-term impacts on core and critical clinical services. If the impacts of COVID-19 last longer than six months as expected, healthcare systems should start to assess the use of IoT and other digital technologies to augment and enhance current practices. For example, the use of 'virtual clinics', building on existing telehealth initiatives, with health wearables and phone-based apps using 'chat bots' to detect and record patient data on a regular basis has been suggested, to reduce clinical load, improve chronic disease monitoring and provide community engagement and communication (Ting et al., 2020). However, the ramifications of increased data collection in the deployment of these types of initiatives will be important for governments and healthcare systems to consider, to ensure that they are proportional to their efficacy and citizen expectations of privacy. These issues are discussed in more detail in section 3.6.2.1.

2.5.10.2 Regulatory considerations

Future opportunities include integrating digital health records and emerging health innovations with and between different IoT devices. To realise the potential in Australia, national bodies such as the Australian Digital Health Agency, the Department of Health, Australian Institute of Health and Welfare or the Australian Commission on Safety and Quality in Health Care could consider developing a strategy that assesses IoT health applications from a clinical implementation perspective. The strategy could outline areas for further R&D and provide appropriate regulation on how to collect and store health information safely, with consideration of who controls the data and the level of control of the individual. A clear code of practice on the management of data, privacy, confidentiality and cybersecurity would be important to transition to a fully realised smart healthcare system (see Chapter 3). It is also worth considering making it mandatory for only certified IoT products to be able to collect, store and communicate healthcare information with healthcare cloud servers (Internet of Things Alliance Australia, 2017d).

2.5.10.3 Architecture requirements

Data management in IoT healthcare applications will be similar to other applications of IoT; however, the data required to monitor the human body will need to be high in fidelity, resolution, volume and velocity. Fog architecture and cloud computing are likely to be required to receive, process, store and communicate these data. Hospitals and clinics will also need to consider employing or consulting with fog specialists to oversee the management of these data (Farahani et al., 2017).

2.5.11 Freight and logistics

Regulatory systems relating to freight and logistics can be complex, spanning issues relating to speed, mass limits, truck dimensions, driving hours and load restraints. Most government agencies have developed comprehensive departmental and agency online regulation repositories. However, it can be difficult to configure operational cloud-based software to incorporate all of these the regulatory requirements. This means there is a high degree of reliance on individuals managing the program software to have a comprehensive understanding of regulatory constraints and apply these during operations. As IoT systems evolve, the number of M2M interactions in business decision making will increase. Companies and governments will need to work together to ensure that domestic and international regulatory systems are interoperable with operational software, with frameworks spanning quarantine and specific commodity declarations, import and export restrictions and import duties.

2.5.12 Smart mobility

2.5.12.1 Mobility as a Service

In 2018, ITS Australia assessed the opportunity to deploy MaaS in Australia, canvassing views from over 80 expert interviews and conducting a customer survey on attitudes towards this transport solution. Most experts agreed that the integration of different transport services was the greatest challenge for MaaS in Australia, given the siloed systems in many regions. Other issues cited included data access and sharing across the private sector, the existing transport ticketing software and payment integration. Some experts considered that the biggest hurdle was the lack of a compelling commercial business case, although opportunities were seen to exist in cities (Intelligent Transport Systems Australia, 2018).

There is an opportunity for governments to act as data brokers, building on the existing work of the ONDC, to facilitate data sharing between different transport providers or create a digital ecosystem to support transport service providers, so that digital infrastructure would not need to be built from the ground up.

National data protocols and standards would be a positive development, with the General Transit Feed Specification developed by Google cited as an example. This has been adopted by the public transport industry as the default format for releasing public transportation schedules and associated geographic information. There is also a case for government oversight to ensure that social equity is considered in any system, for example with a minimum standard of service delivery for populations at risk of disadvantage (Intelligent Transport Systems Australia, 2018).

2.5.12.2 CAVs

Connectivity challenges

A challenge for automotive companies will be selecting the type of network technology that will enable V2X in their vehicle models. Currently, the two leading options are cellular 5G or dedicated short range communications (DSRC) (Yoshida, 2019). As Australia imports most of its vehicles (Department of Foreign Affairs and Trade, 2019), it will be important for governments to consider a technology-neutral approach when developing regulations for V2X, and monitoring international developments in the automotive space.

Data considerations for CAVs

While the IoT consists mainly of static objects and sensors, CAVs will operate as rapid mobile objects within the network structure. This may impact on the transmission of data. Simulations of data transmission rates with an increasing number of cars show significantly variable rates of successful data transmission. Algorithms and protocols that are less sensitive to the number of vehicle nodes will need to be developed, as there will be varying numbers of vehicles in the network at different times and situations. Performance metrics, such as throughput, end-to-end delay and latency for real-time applications will require ongoing research (Ang et al., 2018).

Research is also being conducted using 'Internet of Vehicle' data to find the optimal routing for vehicles to minimise average waiting time to reduce congestion and accidents (Lee et al., 2016). This proposes a mobile fog computing model where vehicles in a vicinity form a local group (vehicular fog) for cooperative computing, in which vehicle contents and services are produced, maintained and used. This leverages the collective processing and storage capacity of vehicles and mobile devices, constructing a distributed computing environment that extends the capability of vehicle interactions (Lee et al., 2016). Internet of Vehicle data are intended to provide services to vehicles through the computing cloud to improve communication with surrounding vehicles and detection of potential hazards (Lee et al., 2016).

A future consideration for the deployment of CAVs in smart cities will be their integration in the Internet of Vehicle and broader IoT ecosystem. For example, there is the opportunity to use vehicles as mobile ubiquitous local area network extensions to opportunistically collect and distribute data in smart environments, such as for air quality monitoring. This type of integration has not been comprehensively explored (Ang et al., 2018) and is still an emerging research area.

Safety

Safety remains a primary concern for CAVs and ongoing research considerations include latency requirements and resilience to security attacks, particularly for safety-based applications such as cooperative collision avoidance systems (Ang et al., 2018). Further work on telecommunications technologies and their utility for different vehicle applications will be required. For example, researchers have demonstrated that advisory speed limit control strategies to improve traffic flow will perform better over cellular networks than dedicated short range communications networks (Ang et al., 2018).

Backward compatibility and legacy issues

Australians, on average, replace their cars every 10 years (Australian Bureau of Statistics, 2019). It will therefore take time before the majority of Australians own cars fitted with IoT technologies. While some work is underway, backward compatibility or legacy issues will need careful consideration as the number of CAVs grows. For example, the challenges of integrating CAVs into existing road safety systems will be a key issue to be monitored and addressed through national initiatives such as the next National Road Safety Strategy for 2021–30. Further, the interaction between new vehicle technologies and existing vehicles and infrastructure is the subject of a number of regulatory and infrastructure projects in Australia, with a view to ensuring that CAVs positively contribute to road safety objectives. For example, the National Transport Commission's automated vehicle project agenda will look at issues such as how automated vehicles should interact with law enforcement and emergency services personnel while in operation.

Further research into consumer acceptability and barriers to the uptake of CAVs in the Australian context, as well as related considerations into the associated changes in employment and community conditions would also be beneficial.

CAVs as a mode of transport in MaaS

CAVs are also expected to be a new mode of transport to support deployment of MaaS. They would be especially useful for the first and last stages of travel. If well planned and implemented, CAVs will allow new business models for car sharing and ride sharing, for example, to deliver passengers to public transport stations or their destination of choice. This would help to overcome issues such as limited accessibility and reliability on public transport, where users can be restricted by distance or limited scheduling (Gao and Kornhauser, 2014). Key challenges that the IoT could assist with are in fleet size optimisation, passenger demand prediction, and providing reliable and timely services to users.

2.5.13 Novel data considerations

The IoT will extend data analytics, commercialisation and governance frameworks into more diverse environmental and industry contexts. These opportunities will need to be balanced against the potential for new asymmetries in data access and re-use by major platform companies as compared to smaller Australian companies and consumers.

It is therefore important that the IoT is not considered in isolation from wider challenges associated with the global data economy. An overly 'device-centric' approach limits the many overlaps between the IoT and broader social, economic and cultural disruptions associated with the advance of AI, automation and platform business models.

Developments in real-time IoT data analytics are likely to lead to a research field in its own right, with a plethora of dissemination and exploitation opportunities. It is expected that the IoT will increase the amount of personally identifiable data (e.g. within a smart city or region's transport systems). As such, accountability-by-design (Crabtree et al., 2018) should be an emerging priority. Data science techniques and provenance schemes will be useful in assisting to quantify the likely completeness, precision and accuracy of data records. Industry-specific opportunities from these developments are likely to include:

- computing professionals and technology companies developing and producing new IoT hardware and software solutions
- telecommunications professionals developing the data communication networks that support IoT hardware
- data scientists working on ways to effect data collection, data wrangling and analysis
- city planners, commercial organisations and advertisers using location-based services.

With the transition to new IoT data search engines and service discovery, flexible interactions between IoT and edge devices may be created, such that the primary providers and hosts of information become evenly spread through the internet.

In addition, there are opportunities for government organisations to participate more in information storage and processing of these data in smart cities and regions. This may include assessing obligations to retain data under the *Archives Act 1983* (Cth) in relation to Commonwealth records that may be generated by the use of IoT, as well as relevant state and territory archives legislation requirements.

2.5.14 Augmented reality and virtual reality

AR can extend IoT experiences of the real world toward virtual environments and reality. It has been suggested that pervasive AR in public spaces may raise ethical questions (McEvoy, 2017), including questions about who has the right to augment the environment, as well as concerns about privacy and anonymity. It will be important to facilitate discussions regarding the desire, necessity and quality of integrating IoT technologies to blend virtual and real environments to the degree that they are indistinguishable from each other. Regulatory frameworks may be required to assist the public to distinguish virtual and augmented content from real content in future.

CHAPTER 3 ACCEPTANCE AND TRUST – CONSIDERING SECURITY AND PRIVACY

Chapter overview

Short-term

- Governments should provide leadership to help consumers and industry to understand the security and privacy risks associated with IoT technologies. This could include engagement with manufacturers and service providers to develop secure-by-design thinking for the entire lifecycle of IoT products.
- Australian and state and territory governments could also consider whether current legislative measures in Australia cohesively establish baseline protection responsibilities or mechanisms for redress where a privacy breach due to IoT has occurred.
- Further research on emerging security and privacy risks and their potential impacts, including options to address these would be beneficial.
- The Australian Government could consider whether enhanced surveillance powers are consistent with international human rights obligations in light of COVID-19. While there is some leeway to adopt specific measures in the current crisis, testing initiatives for necessity and proportionality is important.

Medium-term

- Australia should continue to be proactive in its approach to security and consider establishing baseline protection and redress mechanisms, noting that new risks will continue to arise. The security of IoT systems will be dependent on the quality of the decision making software and digital networks that support these applications. In particular, this should apply to sectors with higher requirements for security such as healthcare and government.
- Security solutions will need to cater for an ecosystem where IoT devices with unpatched vulnerabilities will often be present in the network infrastructure, co-existing with other devices during the device lifetime. Where upgrade paths are impossible, or if an undue burden is placed on the end user to upgrade the IoT device's software and security, device manufacturers may have to get it right first time.

- As the IoT becomes more pervasive, it will be difficult to both build consumer awareness of the necessary frameworks and risks and to extract informed consent for mass-distributed styles of data-collection. Action is required to ensure that data collection, usage and application is safe, ethical, meaningful and fit for purpose, supported by appropriate legislation and regulatory frameworks. To support this, national data standards that are consistent across states and territories could provide guidance on the definition, capture, analysis and reconciliation of data. The standards should aim to ensure that data are appropriately used and shared, to enhance service delivery outcomes across all Australian governments.

Long-term

- It may not be sufficient to certify components or products in IoT security systems in the future. The certification of monitoring of whole systems should be considered by industry and governments.
- The threshold for ensuring a customer is sufficiently informed in the future may be higher, particularly for complex IoT product-service packages.
- The degree to which Australian employees will be able to negotiate restrictions on the use of IoT devices in the workplace will vary significantly on a case-by-case basis, and regulatory guidance may be required to provide certainty as to the allowed limits on such IoT deployments.
- Australia should continue to monitor and identify ongoing data use and practices related to IoT applications and strengthen any frameworks to ensure ongoing community trust as necessary.

3.1 Introduction

IoT technologies will challenge our understanding and expectations of security and privacy in a hyper-networked sensory environment. The size and ubiquity of these networks will increase the number of cybersecurity threats and the volume, veracity and speed of data that will be collected. The interdependent relationship between security, privacy and the use of IoT should be assessed critically by governments and industry in order to meet community expectations. The discussion below demonstrates the inherent complexity of this technology, as it becomes increasingly embedded into society's processes and systems. These are further expanded upon in Appendix C (Security) and Appendix D (Privacy).

Over the next decade, the Australian Government should continue to monitor and identify emerging security and privacy challenges related to IoT applications and strengthen any frameworks as necessary. One-off solutions will likely be insufficient to deal with the continuing evolution of emerging technologies such as the IoT, so effective mechanisms in law and policy would be beneficial to satisfy community expectations. This could include pro-active and swiftly reactive policy and rule-making bodies and processes, the use of appropriate language and interpretative principles in legislation and judicial decision making, and well-resourced, informed and activist regulators.

3.2 Security

One of the biggest security challenges with IoT systems is the substantial increase in the number of surfaces available for security attack. At present, many IoT devices do not have any security functionality (Martínez et al., 2016); even for the ones that do, the security measures are often primitive and can be easily subjected to attacks. Compromising one or more devices in the infrastructure can lead to proliferation of malware and attacks, potentially leading to the compromise of the whole network system.

3.2.1 IoT system vulnerabilities

3.2.1.1 Distributed systems

IoT devices usually contain an embedded processor with onboard software and will often be connected through a number of intermediary connections (including cloud services, telecommunications networks and local networks); they can be connected to networks via different providers and can use several different connectivity strategies at once, such as wireless and mobile networks (IBM Analytics, 2015). These factors make them susceptible to a range of security vulnerabilities and threats, not only through the device itself but also through the systems to which they are connected. Risks emerge from the IoT through insecure network services, interfaces, software and firmware. Insufficient encryption, authentication, authorisation, security and physical safeguards are also security issues.[27] Mitigating risk is also challenging because it involves assessing each layer for vulnerabilities (Palmer, 2018).

3.2.1.2 Complex upgrade pathways

A common solution for software vulnerabilities is to regularly patch them. However, to secure an IoT system by applying security patches, it may be necessary to obtain authorised access to all the relevant interfaces. Device manufacturers may be unable to do this on behalf of users, users may not register their devices with the

[27] This is a consolidated list adapted from the Open Web Application Security Project, Top 10 IoT Vulnerabilities (2014) Project Open Web Application Security Project Wiki, cited in Manwaring (2017b).

manufacturers, upgrades may require high engagement from users, or users may simply leave old and disused devices within networks with outdated software. This can make it difficult to ensure the security of a system.

3.2.1.3 Lack of security-by-design incentives

In some business applications, the cost of implementing security may outweigh the resulting benefit. Suppliers with low profit margins and limited experience in manufacturing computing products may have little incentive or capability to ensure that IoT devices operate reliably. As noted in section 1.5.3, consumers may have preferences for convenience over security. Due to the wide array of functionality and design purpose in IoT devices, it may not be clear to manufacturers and/or consumers how security breaches could cause harm (i.e. an IoT heart monitor has clear risks and need for security, whereas a smart IoT fridge has less tangible security risks for consumers). Further, it may not be cost effective for device manufacturers to provide software patches in a timely and regular manner.

Security solutions will need to cater for an ecosystem where IoT devices with unpatched vulnerabilities will often be present in the network infrastructure, co-existing with other devices during the device lifetime. Where upgrade paths are impossible, or if an undue burden is placed on the end user to upgrade the IoT device's software and security, device manufacturers may have to get it right first time (Brumaghin et al., 2017). This is in conflict with the increasingly dominant 'agile' approach to software development that encourages a more forgiving process of iteration and continuous improvement (Nguyen et al., 2017).

3.2.1.4 Cyber-based crimes

Cyber-based crimes, such as those enabled by the increasing ubiquity of IoT devices, have been described as the ideal attack vector for malicious actors (Jenkins, 2016). The security vulnerabilities in IoT systems can lead to a number of adverse outcomes:

- Individual devices can expose a whole system: device-level vulnerabilities can allow attackers to insert backdoors or Trojans into a network.
- Data poisoning can alter machine learning: if machine learning algorithms are being trained at the back end using the data collected from IoT devices, then tampering with data can fool or cheat the machine learning algorithms used in decision making. Attackers may insert or manipulate data into IoT systems, allowing them to adversely affect performance or cause targeted misclassification. The compromise of data integrity could have a particularly detrimental effect if data from IoT devices are used in government decision making.
- Data breaches can cause harm: data breaches may impact end users, especially where the data or outcomes are sensitive. Attacks on medical IoT devices, such as heart pacemakers and implants, can enable settings to be changed leading to adverse health effects. Attacks on smart electricity infrastructures can lead to malicious attackers stealing electricity or even potentially causing blackouts to large parts of a city or regional area. There have been numerous examples of IoT devices that have been vulnerable to breaches including smart city lights (Correa, 2016); security cameras (Buntz, 2019); shipping scanners (Kovacs, 2014); smart home hubs (Whittaker, 2019); smart televisions (Consumer Reports, 2018); medical devices (Zetter, 2015); children's toys (ForbrukerRadet, 2016); location trackers (Franceschi-Bicchierai, 2016); and cars (Greenberg, 2015).

3.2.2 Impacts of security attacks

At their worst, attacks can have devastating effects on businesses and critical industries, threaten national security, and even directly or indirectly affect human lives. Some data and violations have been more sensitive than others, such as breaches in domestic settings. It may not be enough for manufacturers of individual products to certify, maintain or patch the components independently, instead there may be a need to monitor whole systems in place. IoT security is likely to need to move from single products to end-to-end solutions and eventually to the entire security architecture.

Further information on the types of IoT security breaches and mitigation techniques can be found in Appendix C.

3.3 Opportunities and challenges

As the deployment of IoT devices in smart systems continues to increase in different sectors such as smart cities, transportation, agriculture and healthcare, there is a need to ensure that the devices meet certain minimum security standards. Multi-layered IoT systems can make it unclear who is responsible for designing and implementing overall system security, installing system upgrades and policing vulnerabilities. The IoT can also make it challenging to obtain authorised access to a system to trace, test or fix these issues.

3.3.1 Establishing baseline protection and redress mechanisms

Australia should continue to be proactive in its approach to security and consider establishing baseline protection and redress mechanisms, noting that new risks will continue to arise.

In late 2019, the Australian Government released a proposed voluntary industry *Code of Practice: Securing the Internet of Things for Consumers* for public consultation, to promote the production of 'secure by design' devices. However, as these standards are voluntary, compliance is not guaranteed. It is important that this work is therefore complemented with policy initiatives to educate consumers about the risks of unsecured devices so that they can be better informed in the purchase and use of IoT devices.

Over the next decade, the security of IoT systems will be dependent on the quality of the decision making software and digital networks that support these applications (Batty, 2013; Kitchin, 2013). Security should be assessed not only in respect to government use but also for businesses and consumers. Regulators may need to consider the following:

- leadership by Australian governments to support community understanding of the security risks associated with IoT technologies
- engagement with manufacturers and stakeholders to ensure an appropriate level of protection from unauthorised access, control or interference for applications
- many IoT devices have limited computational resources, sometimes without text-supporting interfaces such as a screen
- security guidelines and policy management need to be light-touch and adaptable, to be applicable to billions of devices in a heterogenous environment and to allow for technological development
- regulatory processes may need to include some form of independent penetration testing of products that contain software as part of the approval process (not solely relying on the manufacturers' guarantees)

- it may not be sufficient to certify components or products in a system; certification and monitoring of whole systems may be needed
- the impacts of smart system failures and how much data and intelligence may be exposed
- software resilience and redundancy
- robust end-to-end system maintenance.
- Monitoring overseas developments in security and sourcing technology

Many current and future IoT technologies involve generating highly sensitive personal data in private spaces such as the home, as well as in public spaces such as schools, health services, workplaces and transport systems. The increased use of IoT technologies by Australian businesses and government agencies could also open these entities to threats to their data security that could disrupt their commercial interests or service delivery. It is important for the Australian Government and industry to monitor ongoing overseas IoT developments in security, and to be mindful when sourcing technology solutions from overseas companies, as there may be competing security and privacy interests. Participation by the Australian Government and industry in international standards committees or groups that monitor security and privacy interests (such as through the Australian Government's participation through the ITU and Standards Australia's participation through the International Organization for Standardization) will be important to monitor and manage our interests in this regard.

3.4 Privacy considerations

Privacy management in the context of IoT systems primarily addresses the privacy of data. That is, data from IoT devices should not be revealed to unauthorised users and, more importantly, a user should have control over the level to which their own data are collected by IoT devices. Today, personal data are created, transmitted, tracked and recorded across multiple platforms. The level of detailed, real-time, location-based data also represents the biggest cause for concern (Neumann, 2015), as there are significant risks and implications for consumer data privacy. For citizens to obtain the full benefits of IoT-enabled smart solutions, they need to be able to feel that their data are safe (Crist et al., 2015). As the use of devices becomes more widespread, it is likely that a greater quantity of data, including data that are more intimate and personalised in quality, will be collected and processed. However, users' knowledge is often limited about what and how much data are being collected, the uses of data, who is receiving the data, and for how long data are being used. Information on the assessment of Australia's current privacy regime can be found in Appendix D.2.

3.4.1 Consumer understanding and consent

Customers have a right to sufficient, accurate and intelligible information on the nature, features and dependencies of a product or service before they enter into a contract, so that they can make an informed choice. When an end-user accepts a supplier or provider's privacy policy, they enter into a contract, consenting to that vendor's use of their data, which may include sharing it with third parties. While this is not limited to the IoT, the greater the amount of data made available by IoT devices, the greater the likelihood of suppliers and providers requiring data as a mandatory component of the supply contract. In future, the threshold for ensuring a customer is sufficiently informed in the future may be higher, particularly for complex IoT product-service packages.

3.4.2 Content

Content knowledge relates to consumer understanding of what a device does, and what they are allowed to do with it. Knowledge of 'normal' functionality, that is, the capabilities that a device is expected to have when bought by a consumer, is usually insufficient, particularly for IoT devices with volatility and system dependencies.

Many IoT devices are hybrids of object, software, hardware, service(s) and functionality, which often require associated services, such as access to cloud data handling facilities and website interfaces. A complex network is likely to exacerbate complex contractual arrangements and liability allocation for IoT-specific contracts. Even a basic IoT device may require many separate contracts dealing with hardware, software development, software licences, installation, website and app usage, payment services, connectivity provision, sale, distribution and rental. For example, while a smart home device may be with one supplier, the addition of any programs or applications for added functionality could mean separate contracts. Contracts may be with separate entities, with some having no connection with (or knowledge of) others in the network. The complexity of contractual arrangements within a network can make it difficult to identify all applicable contracts, let alone interpret them for end-customers (including enterprises) and network actors.

Clear information on price is fundamental to any customer contract. This includes not just the price of initial supply but also follow-on costs, such as purchase of additional applications, subscription fees for service agreements and costs of consumables. Customers should also be aware of non-money considerations, such as post-supply obligations, for example in relation to data and use restrictions.

The dependence of IoT devices on interaction means that information about interoperability is also often critical. Particular systems may only allow add-ins of particular brands of IoT devices, thereby restricting customers' freedom of choice, resulting in vendor 'lock-in'.

3.4.3 Intelligibility

An additional information challenge inherent in complexity is that customers may not be able to make well-informed decisions when they are given information that is incomplete, misleading, overly complex or too voluminous. Opaque wording and technical terms are the norm for software and hardware contracts, and initial research indicates that this has not changed for IoT devices. The content provided may be accurate, but if it is not intelligible to the average customer, it is insufficient to enable an informed choice.

Careless drafting can be an additional problem. Researchers have identified terms and conditions in contracts involving IoT devices that contain wording obviously written for older technologies, or wording drafted for one jurisdiction in contracts made for another. To counter these issues, privacy policies must be clear and intelligible. The Office of the Australian Information Commissioner (OAIC) provides guidelines on developing privacy policies requiring certain entities classified in the APPs to develop a policy that is in language which is easy to understand and an appropriate style and length (Office of the Australian Information Commissioner, 2019a).

3.4.4 Consent in smart cities and regions

In smart cities and regions, smart buildings or smart retail spaces may track an individual's location and activity to provide customised experiences based on the user's context. Such services could include customised heating or air conditioning controls based on user preferences, services to help locate nearby resources or the delivery of customised coupons or incentives in the retail setting. However, capturing fine-grained sensor data also raises concerns about building owners being empowered to use the data captured to further infer properties such as personal habits of individuals – properties that individuals may not be comfortable sharing without explicit consent.

Opt-out approaches to consent are a possibility, but while these approaches are not prohibited under Australian law, it is often difficult to establish whether informed consent was granted (Office of the Australian Information Commissioner, 2019b). This is compounded when IoT devices are deployed in public or shared spaces. Smart city trials include no surveillance-free zones at all (Goodman and Powles, 2019). Where IoT devices are deployed by private entities, public oversight may be diminished.

Mechanisms for informing users about policies related to the collection of data in smart spaces, as well as mechanisms for obtaining user consent, would help to address some of these concerns. Such mechanisms could be designed to protect users from malicious IoT spaces that may capture data other than what has been agreed to in the policy. This could help empower users to retroactively attest policy compliance in the IoT space.

Scenario 3: Privacy, security and cyberhygiene

The Singhs have gone on a family holiday to Rottnest Island. Priya Singh is comfortable about leaving her home for a few days. Her connected IoT home platform activated the security system five minutes after the Singhs left home, once the sensors in the home detected no movement. This was also correlated with GPS location data from the Singh's smartphones and Priya's activity bracelet. As a result, cameras at the front and back of the property turned on and activity sensors started to track for any suspicious movement.

Fifteen minutes into the ferry ride, however, Priya gets a notification on her phone that the smart refrigerator has been opened. She immediately opens up the security camera app to view footage within the house but receives a notification that the cameras have been turned off. Alarmed, the family return home as quickly as possible. On their arrival, they find that they cannot get into their home and the automated smart lock won't let them in. The Singhs quickly call the police. Jai finally recalls where he left an emergency key to the back-veranda door. The key hasn't been touched in the two years since their home was connected.

The police arrive and on further investigation by the Cybercrimes unit, the Singhs are informed that their connected refrigerator was hacked into by an unauthorised user, who then gained access to their connected IoT home platform. The Singhs are shocked. When they call the refrigerator manufacturer, they are informed that they did not register the appliance to receive security updates once it was connected to their home network. This allowed the hacker to access their network via the compromised refrigerator and subsequently gain access to their security system. Jai recalls archiving the reminder to register the refrigerator after being distracted by its smart water temperature capabilities.

The Singhs' experience has been sobering. Priya and Jai now take more care in the management of their IoT devices and the importance of cyberhygiene, such as making sure all devices are registered for security updates.

3.5 Surveillance and privacy

3.5.1 Surveillance in public spaces

There are substantial implementation challenges concerning how public smart infrastructure could augment monitoring of people without comprising confidentiality for conditions that remain highly stigmatised and place real limitations on work and lifestyle options (e.g. ability to secure insurance, opportunity to work in certain occupations). Explicit consideration should be given to what is lost when public spaces become managed and subject to continuous surveillance or monitoring, in terms of the ability and rights of individuals and groups to associate and define the uses of those spaces. Rational algorithms reduce the potential of public space as a theatre for 'chance encounters' (Risom et al., 2016). Explicit 'privacy zoning' could be used to define – and socially signal – limits on the types and extent of IoT-enabled monitoring deployed in specific locations.

3.5.2 Surveillance in the workplace

The right to work includes the rights to 'free choice of employment, to just and favourable conditions of work and to protection against unemployment' (Article 23(1), Universal Declaration of Human Rights, 1948). The use of IoT devices in the workplace may challenge these rights and introduce conflict between an employer's interests in operational efficiency and oversight, such as performance monitoring, against an employee's security protection and right to privacy. However, the IoT may also improve employee protection by monitoring employer compliance with health and safety obligations and workplace abuses. Research on this issue is currently limited and warrants further investigation.

There is an emerging contested terrain in the relationship between the IoT and employment, particularly as the technology becomes more pervasive (Holland and Bardoel, 2016). The use of technology to increase electronic monitoring and surveillance of employees has raised significant concerns (Holland et al., 2019). As well as eroding the power balance, the deployment of IoT surveillance systems also threatens to erode trust. The degree to which Australian employees will be able to negotiate restrictions on the use of IoT devices in the workplace will vary significantly on a case-by-case basis, and regulatory guidance may be required to provide certainty as to the allowed limits on such IoT deployments.

Case study 22: Facial recognition technology

As part of the Switching On Darwin project, 138 CCTV cameras with facial recognition capabilities were installed alongside public Wi-Fi, new lighting and sensors. There have, however, been community concerns about this part of the project, and the risk of erosion of privacy through intensified surveillance (Sadowski et al., 2020). Darwin Council reported that there was no public consultation on the technology's use prior to the submission funding application (Ashton, 2019). In response, the Darwin City Council has announced it would conduct a privacy impact assessment on all new technology and that more public information sessions would be held in the future (Adams, 2019).

This case study demonstrates the importance of early and proactive stakeholder engagement prior to the implementation of potentially contentious IoT technologies such as facial recognition or surveillance.

Case study 23: Biometric data employee monitoring

In the case of *Jeremy Lee v Superior Wood Pty Ltd* [2019] FWCFB 2946, a sawmill introduced fingerprint scanners to monitor employee work hours. When the employee Jeremy Lee refused to comply and hand over this biometric (fingerprint) data, he was dismissed by his employer.[28]

Collection of sensitive information under the Privacy Act is prohibited, unless an individual consents to the collection of the information and the information is reasonably necessary. Superior Wood's notice on this collection was framed as a directive rather than a request, as the directive stated that disciplinary action would be taken for those that refused to comply. The dismissal was overturned on appeal at the Fair Work Commission, stating that this directive was unlawful, because any 'consent' would not be genuine as it would be vitiated by the threat of disciplinary action. Superior Wood was ultimately found to have made several breaches of the Privacy Act.

As this case demonstrates, lack of understanding and relevant risk assessments of IoT in the workplace can lead employers to prioritise utility over worker protections.

3.6 Opportunities and challenges

IoT systems have many interwoven parts, consisting of service providers, network administrators, platform operators, device manufacturers, users and participants all contributing to a complex network. In addition, the predicted substantial increase in IoT-enabled devices over the next 10 years will lead to greater volumes and velocity of data, particularly as IoT applications become more pervasive in society. These issues will make it challenging for consumers to sufficiently understand privacy risks: what and how much data are being collected, the uses of data, who is receiving the data, and for how long data are being used. The threshold for informed consent will be higher, particularly for complex product-service packages or for mass-distributed styles of data-collection, such as for public service delivery using IoT.

In the short term, engagement with the community is important to build understanding and awareness of the privacy risks that IoT technologies can pose. Incremental and proactive engagement can help empower community members and assist in building digital literacy to meet emerging privacy challenges as they arise. To also ensure community trust and acceptance, governments and workplaces may have greater responsibility to be transparent and accountable in the collection and use of data. Research to understand and assess emerging privacy risks and impacts to supplement this work would be useful, as well as identifying potential options to assess these issues. This will also enable greater community trust.

Over the next decade, there is a role for governments to ensure that data collection is safe, ethical, meaningful and fit for purpose, supported by legislation and regulatory frameworks. This should include monitoring ongoing data use and practices related to IoT applications and strengthening frameworks as necessary. Areas for focus are outlined below.

[28] Biometrics refers to technologies that measure and analyse unique and distinctive characteristics of an individual (Moradoff, 2009).

3.6.1 National data standards

At the national level, the ONDC is currently undertaking work to reform how public sector data is shared to improve service delivery, policy development and research. Current work includes the development of the Data Availability and Transparency legislation, which aims to streamline and modernise public sector data sharing, with the ONDC facilitating greater transparency of data sharing activities through registers of data sharing agreements and data users (with trusted accredited users and service providers).

Building on this work, national data standards that are consistent across states and territories could provide guidance on the definition, capture, analysis and reconciliation of data. The standards should aim to ensure that data are appropriately used and shared, to enhance service delivery outcomes across all Australian governments. This could also complement existing work developed by the Australian Government such as the Data Sharing Principles and the Consumer Data Right, as well as the current data sharing frameworks of state and territory governments.

In addition, increased data collection is also likely to lead to new asymmetries in data access and re-use by major platform companies, compared to smaller Australian companies and citizens. The Australian Government could consider regulating the ownership, usability, availability, security, integrity and commercialisation of data by industry as IoT applications extend further into diverse industry contexts and supply chains over the next decade.

3.6.2 Monitoring and surveillance

Individuals have a need for privacy, and clear boundaries are required on what data are revealed to the employer and associated third parties (Fairweather, 2017; Petronio, 2002). Importantly, the IoT can introduce new forms of tracking which go beyond the individual's ability to manage their privacy. It will be important to educate community members, managers and employees of the implications and impact of this new era of the IoT, to protect against power imbalance and privacy violations.

3.6.2.1 Increased surveillance and data collection in national health emergencies

The current emergency relating to the COVID-19 pandemic as of August 2020 has led to a significant increase in the collection of information relating to the location, health and habits of individuals, both by the Australian and state governments and most likely by private organisations providing services to government. This trend is likely to continue and extend its reach, particularly in light of other countries' activities in isolating and tracing contacts of infected individuals, and in strict enforcement of quarantine restrictions. For example, Singapore has introduced geolocation tracking of the smartphones of individuals in isolation in order to enforce 'stay-at-home' notices (Sharwood, 2020). The University of South Australia is currently promoting its research work on a pandemic drone with computer vision capabilities allowing the detection of temperature, heart and respiratory rates, and people sneezing or coughing in public spaces (University of South Australia, 2020). Many other IoT devices with elevated capacity for the collection of highly personalised and intimate data may also be used in the fight against COVID-19.

Part VIA (dealing with personal information in emergencies and disasters) of the Privacy Act allows for the lifting of significant protections around personal information during emergencies. Many, if not most, individuals in Australian society may be happy to temporarily suspend privacy protections to aid in reducing the spread of COVID-19.

However, the protection of that information from malicious actors during the pandemic and the potential use of that information by government and businesses once the emergency is over is important to consider. For example, some private organisations with poor privacy records have been in negotiations with overseas government agencies around the provision of surveillance tools to help halt the spread of COVID-19 (Grind et al., 2020), giving rise to the possibility of inappropriate profiteering from that data. The lack of a clear right to erasure of data in Australian privacy law is likely to prove problematic in this context, similar to other like jurisdictions (Gunasekara, 2020).

The Australian Government could consider whether enhanced surveillance powers are consistent with international human rights obligations. While there is some leeway to adopt specific measures in the current crisis, testing initiatives for necessity, proportionality and scope creep is important. Governments and public health experts may need to ensure that monitoring initiatives are effective and narrowly tailored, minimising the amount of data that is collected in order to achieve legitimate and defined goals (Funk, 2020).

As noted in ACOLA's research (Walsh et al., 2019), increased perception of surveillance can alter behaviour, even when faced with only the possibility of being under surveillance. This can include people avoiding talking or writing about sensitive or controversial issues, which not only has a 'corrosive effect on intellectual curiosity and free speech' but inhibits the kind of democratic discussion necessary for a free society (Munn, 2016). It will therefore be important for the Australian Government to consider any impacts of enhanced surveillance on civil society and public debate.

Transparency and accountability are crucial to helping citizens understand how and why their privacy rights are being impacted. Transparency about how data is collected, processed and shared must be prioritised to gain public trust and acceptance. This will ensure that institutions that are responsible for using these powers to monitor and limit the outbreak maintain public trust.

In addition, consideration should be given to incorporating unambiguous sunset clauses so that surveillance or monitoring mechanisms cannot unduly continue once the pandemic ends. Firewalls could be used to contain information from other government or commercial uses, and information be destroyed once the purpose for use has ended (e.g. the pandemic is brought under control) (Funk, 2020).

3.6.3 Evaluating existing legal and regulatory frameworks

It is important for the Australian and state and territory governments to consider whether current legislative measures in Australia cohesively establish baseline protection responsibilities or mechanisms for redress where a privacy breach due to the IoT has occurred. While many IoT devices may be covered under the Privacy Act, as it is technology-neutral and principles-based, new and novel IoT applications may create challenges that will test existing legal and regulatory regimes. Current state and territory policy and legislation on privacy is complementary to the national approach, and it is recommended that this is proactively reviewed to ensure national consistency. For example, research demonstrates that problems are likely to arise in one or more of these four categories in relation to existing legal and regulatory frameworks:

- uncertainty of application
- over- or under-inclusivity
- obsolescence of existing frameworks
- new harms that have not yet been addressed (Bennett Moses, 2007).

The forthcoming review of the Privacy Act will be a useful assessment of the current legislation and may provide a needed opportunity for the Australian Government to consider the four categories above in relation to the IoT. While the OAIC received an additional $25 million in funding in 2019 over three years, ongoing and regular assessment of the resourcing and functions of the OAIC over the next decade would be prudent, as IoT and other emerging technologies mature, and new data and privacy issues arise. More information on existing regulations can be found in Appendix D.2.

3.6.3.1 Recommendations for review of existing legislation

Some of the ACCC recommendations for reform in the Digital Platforms Inquiry are relevant to data-based harms arising in the context of IoT devices and systems. Properly implemented, they are likely to be helpful in addressing some of the above concerns. These recommendations are listed below.

In the *Privacy Act 1988 (Cth):*

Recommendation 16(a):

- broader definition of 'personal information'

Recommendation 16(c):

- the imposition of an informed consent requirement, in particular where collection, use or disclosure of the data is not necessary for the performance of a contract (or as a result of a legal or public interest reason)
- the introduction of default settings for consent that are pro-consumer and not bundled

Recommendation 16(e):

- a direct right of action for individuals

Recommendation 18:

- greater information requirements that align more closely to what consumers want to know, including a requirement that the name and contact details for each third party to whom consumers' personal information may be disclosed to
- more sophisticated user control, including the use of personalised and global opt-in and opt-out controls
- additional restrictions on children's personal information collected or used for targeted advertising or profiling purposes.

In the *Competition and Consumer Act 2010 (Cth):*

Recommendation 21: further prohibitions on unfair practices, including:

- collection or disclosure of consumer data without express informed consent
- inducing consent by 'relying on long and complex contracts, or all or nothing click wrap consents, and providing insufficient time or information that would enable consumer to properly consider the contract terms.'

CHAPTER 4
DEPLOYMENT AND SUSTAINABILITY CONSIDERATIONS

Chapter overview

Short-term

- It is important to consider the ongoing assessment of existing policy and regulatory frameworks prior to the development of any new regimes to prevent duplication of efforts and outcomes.
- IoT applications over the next few years are likely to be supported by existing 3G alongside a hybrid 4G/5G network. It is likely that existing network infrastructure will support most IoT deployments over the next two to five years.
- It is predicted that in the next two to four years, several interfaces between IoT platforms will be developed for increased compatibility and interoperability. However, there are likely to be opportunities for Australian companies to capitalise on niche areas in this space.
- Energy efficiency strategies should not solely rely on technological change but could be complemented by strategies that involve reducing consumption to minimise associated environment impacts. Deployments should be accompanied by education, awareness and behavioural change strategies on the consumer side.
- The Australian Government and industry bodies could continue to participate and progress national interests in international standards committees worldwide as these develop.

Medium-term

- It is important to consider a flexible and principles-based approach to any national regulatory development to ensure that these remain relevant and consistent with future international direction.
- There should be ongoing focus to ensure harmonisation of technological standards across state and territory jurisdictions to ensure that CAVs can operate across long distances and jurisdictional borders.
- Industry predictions suggest that national-scale 5G networks to support these use cases will emerge in the mid-2020s.

- The next generation of telecommunications, tentatively characterised as 6G, is in its embryonic stage. As this technology develops, there are opportunities for Australia to participate in international discussions on the global developments.
- Efficiency evaluations should account for how technologies will likely be used in practice, and shift focus from individual products to networks.

Long-term

- In the future, interoperation will be needed at human semantic levels rather than pure technical levels, so that consistency in the knowledge derived from data with the IoT can be checked at human-relevant levels of interaction.
- It is conceivable that by 2050, the IoT could consume between one and five percent of the world's electricity. Governments and industry could consider measures which seek to achieve lower-energy digital lifestyles, while integrating new IoT devices.

4.1 Introduction

This chapter outlines some of the key enablers for deployment of the IoT in Australia, including the development of standards and network infrastructure that will enable the connectivity required for broad deployment. In addition, it describes environmental considerations for addressing sustainability concerns related to an increasingly device-centric society.

Although it is difficult to forecast what a domestic IoT sector will look like over the next decade, given that novel applications will likely emerge, a number of niche areas based on research and consultation with key domestic and international experts have also been outlined.

4.2 Standards

Regulations are 'any rule[s] endorsed by government where there is an expectation of compliance. It includes legislation, regulations, quasi-regulations, and any other aspect of regulator behaviour that can influence or compel specific behaviour by business and the community' (Department of the Prime Minister and Cabinet, 2020). In its 2019 Human Rights and Technology Discussion paper, the Australian Human Rights Commission broadly classified regulations as:

- legislation: rules mandated through Acts of Parliament and other subordinate legislation under those Acts
- co-regulation: rules, codes or standards defined by industry, which can be enforced if mandated through legislation
- self-regulation: standards, guidelines and policies developed and voluntarily committed to by industry or a sector; sometimes referred to as 'soft law' as they are usually not legally binding (Australian Human Rights Commission, 2019).

For emerging technologies, it can be useful to think about regulations as the baseline for what is deemed acceptable in terms of design, manufacture, function and use. Regulations have relied on relatively closed systems to deliver specific policy outcomes (Australian Communications and Media Authority, 2015), but there are particular challenges for the IoT, given that it envisages global mass connectivity where 'network, device, information and people' are no longer in a closed system (Australian Communications and Media Authority, 2015). This could limit the effectiveness of any nationally developed regulatory schemes because of the increased need for international cooperation and collaboration in the application of this technology (Australian Communications and Media Authority, 2015). In addition, 'the level of reliability needed from a single type of technology may vary, depending on the context of use and its impact' (Australian Human Rights Commission, 2018a, p. 38). For example, there may be a need for greater regulatory oversight in healthcare, where the potential impacts and harms towards individuals could be much greater compared to other areas such as industrial automation.

Current standards are heterogenous, with a multitude of standards applying to different aspects of the IoT (as discussed in section 1.5.1); these represent the different interests of device manufacturers, overseas service providers and standards-making bodies. Aside from technological standards, there is also work being progressed on the social aspects of the IoT, considering the privacy and security implications for end users. Key developments will occur at the international level. Collaboration and cooperation are becoming more common, with industry, international standards-making bodies and governments working towards common goals and greater clarity.[29] Some scholars have predicted that a universal and globalised standard for the IoT network is expected to be finalised in the next 10 years (Barns, 2019a). Stakeholders consulted in the development of this report recommended that industry and the Australian Government continue to monitor developments over the next 5–10 years and continue to participate in international forums where possible to ensure that national interests are represented.

[29] For example, see the Open Connectivity Foundation forum which includes multinationals such as Microsoft, Cisco, Haier and Huawei, and which has forums in China, India and Korea. International standards-making bodies include the ISO and the Institute of Electrical and Electronics Engineers (IEEE), as well as leaders such as the UK or EU.

Stakeholders were also in broad consensus that any development of national standards should be informed by international developments. As with all emerging technologies, the unilateral creation of domestic regulations that are inconsistent with international standards are adverse, severely impacting on Australia's ability to receive, use and operate technology in global supply chains.

4.2.1 National approach to standards

As international standards and industry developments are being progressed, it is important to consider a flexible and agile approach to the enhancement of national regulatory frameworks, to ensure that these remain relevant and consistent with future international directions. Existing human rights frameworks, as well as national and international regulations on data security and privacy provide ample scope to regulate and govern emerging technologies (Walsh et al., 2019), which can be enhanced through using co-regulatory approaches and legislative change where appropriate. A principles-based approach is an appealing option, given the speed of technological advancements that render prescriptive rules obsolete or require burdensome regular amendments. Both government and industry both have a role to play in developing these frameworks.

4.2.1.1 Assessing existing policy and regulatory frameworks prior to the development of new regulations

Existing policy and regulatory frameworks should be assessed prior to the development of any new regimes to avoid duplication of existing effort and outcomes. The ACMA provides useful guidelines to assess existing frameworks and to identify outcomes that may need to be delivered to support the growth of the IoT (Australian Communications and Media Authority, 2015). The following questions could be considered:

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

It will also be important to consider whether:

- existing policy and regulatory frameworks could be extended to include the IoT
- existing frameworks should be lessened
- existing frameworks should be applied in different ways to remain effective problem-solving interventions.

4.2.1.2 Future direction for the development of national regulations

An assessment of the existing regulatory framework for the IoT in Europe found that industry uncertainty about rules, fragmented application of rules across member states and an uncalled for difference in the treatment of different technologies had slowed down innovation and progress in deployment of the IoT, compared to the US and China (Vodafone, 2019). The report recognised that the IoT cut across a range of connectivity technologies and recommended the need for a technology-neutral approach to regulations. This would also ensure that policy developments would not favour one technology or vendor over another but would enable market forces to drive innovation and deployment (Vodafone, 2019). A technology-neutral regulatory framework was proposed, recognising the following principles (Vodafone, 2019):

- proportionality: regulatory burdens should be reduced or eliminated where they are not necessary to achieve the underlying policy objective

- harmonisation: the interpretation and application of any national frameworks should be consistent with international developments to avoid fragmentation of the global market and to reduce compliance costs for IoT providers and users
- neutrality: regulatory obligations should be applied equally and consistently across different sectors, IoT technologies and complementary technologies, such as AI, machine learning and block chain, to avoid favouring one technology over the other
- innovation, flexibility and future proofing:
  - the interpretation and application of a regulatory framework should facilitate innovation, flexibility and experimentation, as well as consider complementary measures, such as using the 'regulatory sandbox' (discussed below)
  - to address potential liability issues, actors across the IoT value chain should ensure contractual arrangements are clear and specify who is responsible where an IoT-enabled product causes damage
- appropriate security:
  - obligations should be balanced against risk and should be applicable across the entire IoT value chain and product lifecycle
  - to promote user acceptance and trust, all participants in the IoT should recognise baseline IoT security best practice principles such as 'security by design'; contractual measures could require trade partners to do the same.

4.2.2 Interoperability

The key challenge for IoT systems will be enabling interoperability over the next decade. Many of the key benefits of the IoT require improved interoperability and data sharing protocols across devices, contexts and networks. This requires a set of universal or common standards for the horizontal architecture of the IoT, including standards for infrastructure, identification, communications, discovery, device management, semantics and data management. This is complicated by the different requirements and capabilities of the IoT across different sectors. For example, the health sector might consider specialised or tailored security standards for IoT health and medical devices, considering the risk of significant harm to individuals. In addition, the lack of standards could lead to asymmetries in use and access by industry. For example, a lack of data protocols can lead to data silos, which can also limit the available insights and efficiencies possible through the integration of data into analytics platforms (Nonnecke et al., 2016). For this reason, IoT technologies are considered to be at a relatively immature stage of development and integration (van Dijck et al., 2018).

Several leading IoT platforms are provided by major technology and data commercialisation vendors, such as Amazon, Google, and Microsoft. These platforms act as intermediary services to connect diverse IoT hardware (e.g. distributed sensors and devices) and application layers. These platforms are designed to act as the 'plumbing' that connects devices and applications. They are usually cloud-based and facilitate the remote management and automation of distributed devices, as well as data management and integration. However, these centralised cloud platforms are expensive, as is the cost of server space for huge volumes of big data. They can also lead to issues of latency in data processing. For this reason, IoT platforms increasingly offer not only cloud-based data integration but also edge-based computing services that facilitate data processing at the local level.

As an IBM report emphasised: 'IoT can be complex, with a large number of suppliers and ecosystem stakeholders needed for success. And the fact that an ecosystem of providers is needed sometimes becomes a stumbling block for many companies – putting IoT into the "too hard" pile' (Sendel, 2019). The high level of heterogeneity operating within an 'IoT stack' reflects the operation of multiple vendors across levels of hardware or 'things', network connectivity, and data analytics and applications. As one paper has noted: 'Interconnecting heterogeneous devices and services provided by different vendors and providing seamless interoperations across the available platforms still remains a big challenge' (Santofimia et al., 2018). Figure 15 represents how the IoT has evolved since 2005. However, open access models for the IoT continue to struggle against the IoT platform offerings by major commercial technology companies. This continues to entrench data asymmetries in marketplaces such as Australia.

In the next two to four years, several interfaces between big IoT platforms are likely to be developed for increased compatibility. Consultation with stakeholders demonstrated that this was reflected in the various regulatory developments taking place across different sectors including transport, telecommunications and consumer protection, depending on the capabilities of existing frameworks to deal with emerging issues from IoT applications.

Similar to the development of standards, interoperability requirements will be driven by international developments. Therefore, frameworks or guidelines to support interoperability must also be flexible and ensure they remain applicable as the technology develops.

4.3 Network infrastructure to support IoT deployment

The network infrastructure and connectivity requirements for IoT will be application specific. Options range from low power wide area network options (LPWAN) for IoT agricultural deployments in rural areas, to industrial automation and telesurgery which may require 5G URLLC on private secure networks or 'campus networks'.

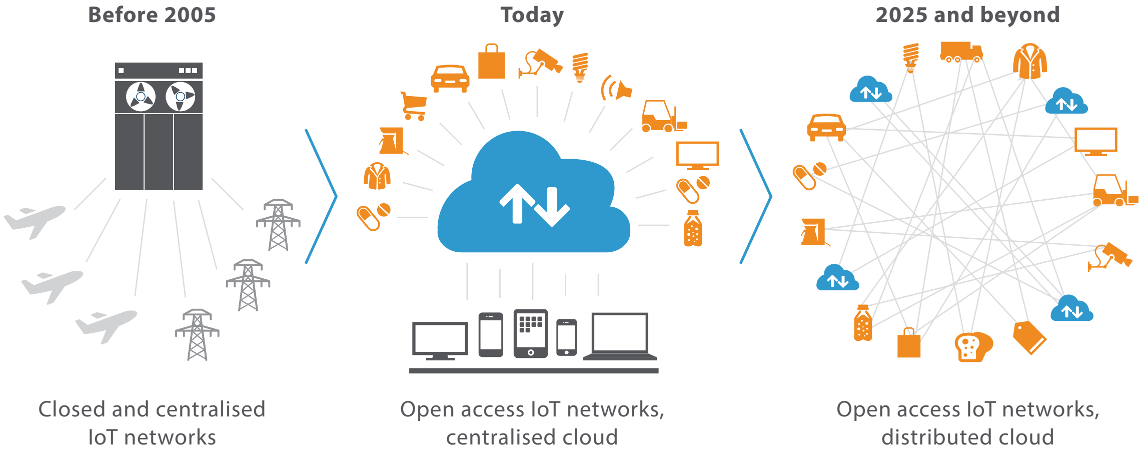

Before 2005
Today
2025 and beyond
Closed and centralised IoT networks
Open access IoT networks, centralised cloud
Open access IoT networks, distributed cloud

Figure 15: A representation of how open access IoT has developed and is likely to develop

Adapted from IBM, 2015.

4.3.1 Wireless communications

Consideration of the specific connectivity requirements for an application is critical, as there is often a vested interest by industry network providers to showcase 'hyped' or unrealistic use cases to promote usage of their network or use cases that may have alternative connectivity solutions. While 5G has been characterised by industry and academic experts consulted in the development of this report as the preferred option for IoT applications, given its speed and low latency, existing telecommunications technologies are also being used to support current deployments of IoT. Ericsson's Mobility Report demonstrated that 2G and 3G connectivity currently enable the majority of IoT use cases worldwide and estimated that there would be 100 million connections in 2019. Ericsson project that Cat-M1 and narrowband-IoT (NB-IoT) will account for 52 percent of all cellular IoT connections at the end of 2025 (Ericsson, 2019). They also project that 28 percent of cellular IoT connections will be broadband applications such as drone solutions and mining and manufacturing applications, with 4G connecting the majority of these (Ericsson, 2019).

These global forecasts demonstrate that a hybrid of connectivity options is likely to support IoT deployment in Australia over the next decade. For example, Telstra estimates that their network provides approximately 3 million square kilometres of LTE-M coverage (LTE, which stands for long-term evolution, is a 4G wireless communication standard; LTE-M is for machine-type communication) for Cat-M1 devices (Loots, 2019) and nearly 4 million square kilometres of coverage on their NB-IoT network (Telstra and Penn, 2020).

The Australian Media and Telecommunications Association has that noted aside from 3G, IoT applications over the next few years are likely to be supported by a hybrid 4G/5G network. Initial (non-standalone) 5G is currently being deployed on existing 4G architecture (Kennedy, 2018). Although more research is required, it is likely that existing network infrastructure will support most IoT deployments. In the early stage of deployment, 5G will co-exist with 4G networks. The main challenge in the 5G rollout will be the transition to high frequency band usage, which enables higher data rates and higher network capacity, but has range, penetration and mobility challenges. Specifically, the 5G deployment will begin in the areas with high network capacity demands, where 4G will provide support for mobility and large area coverage.

Standalone 5G, or 5G that requires dedicated 5G core architecture, will be able to offer the low-latency requirements needed to support IoT deployment in health, industrial automation and CAVs, and for massive machine-type communications designed for wide-area mass applications. It is predicted that industry roll out of national-scale 5G networks to support these use cases will not emerge until around 2025 (Kennedy, 2018). This roll-out is not only dependent on the emergence of use cases to justify the investment but also on the ability of the telecommunications industry to build, access and provide support for numerous new cell sites (Kennedy, 2018). Apart from being deployed in mobile operator networks, 5G is also expected to be used in private networks, such as those in Industry 4.0 or enterprise networking. The Australian Media and Telecommunications Association sees roles for both government and industry to support the roll-out of 5G for public networks. While industry is responsible for building the infrastructure, it is important that there is there is a sufficient spectrum available (in terms of allocation of spectrum and existing licensing arrangements) for a commercial roll-out (one of the key areas of focus in the Australian Government's 5G – Enabling the Future Economy Strategy) (Department of Communications and the Arts, 2017).

Governments can also assist by alleviating community concerns regarding the perceived health impacts around 5G and the deployment of small cell infrastructure in urban areas through initiatives such as the Enhanced EME Program.

The rise of 5G has been predicted to make broadband operators respond with their own investments in faster and higher-capacity networks. This may provide an alternative to 5G for customers who have higher data requirements as data usage grows in the future and may continue to use broadband services (Kennedy, 2018).

The possibility for major carriers to share 5G infrastructure has been raised, particularly as network rollouts reach regional areas (Duke, 2019). This could avoid repetitive construction and lead to improved efficiency and reduced costs. While the Australian Media and Telecommunications Association acknowledged the efficiencies of shared infrastructure in consultation, there has been a historical reluctance for infrastructure owners to share active network capabilities with competitors, unless mandated by government (such as through direction of the ACCC).

4.3.2 Fixed wired versus wireless communications

There are still some scenarios for fixed wired communications in IoT applications (Flammini et al., 2009). These usually occur in private networks or 'campus networks', which consist of fixed wired or wireless communications over a limited geographical area. These are used for applications such as building automation, industrial automation or security cameras/motion sensors for cost and security reasons. There may be an ongoing commercial charge to use a commercial wireless network, whereas on a private network, the ongoing connectivity cost per IoT device is nil. Specific applications of industrial automation may require the use of private networks with URLLC for time-critical processes. For these reasons, for many specific localised IoT applications, it may be preferable to use a private closed network rather than any commercial radio or fixed-line network. In addition, a 'wired' connection may be low cost or free to operate and require no license, compared to higher costs for connections through a commercial wireless network (e.g. 5G or long range wide area network, LoRaWAN), so commercial and cost considerations may also apply. However, wireless solutions may provide higher flexibility, scalability, and less expensive deployment and maintenance. In the next 5–10 years, both wired and wireless communication technologies will be employed according to the different requirements of each application. Mixed wireless networks are discussed further in Appendix B.3.

4.3.3 Satellite communications

Satellite connectivity has already been deployed in use cases where other forms of connectivity are unavailable. LEO satellites can provide low power, low cost and wide range terrestrial coverage, which may be a viable option in RRR areas where radio IoT networks are unavailable. Australian companies Fleet Space Technologies and Myriota, as well as SpaceX, have deployed constellations of these satellites in low orbit space. More information on satellite technology can be found in Appendix B.10.

Case study 24: IoT satellite-modem devices

Beam Communications, an Australian start-up, has developed a new satellite messaging device that automatically switches a mobile device to satellite connectivity when it moves out of cellular coverage. Users maintain messaging capabilities, transitioning from local cellular connectivity to satellite connectivity when required via the Iridium Communications global satellite network. This network provides L-band voice and data coverage to satellite phones, pagers and integrated transceivers globally. The device also includes personal safety features such as location sharing, weather forecasts and real-time worldwide SOS alerts for remote travellers (Tchetvertakov, 2020).

4.3.4 Deployment of 6G

The next generation of wireless communication, tentatively characterised as 6G, is in its embryonic stage. It is envisioned that it could provide data rates of up to 1 terabyte per second and could approach upper limits of millimetre wave radio spectrum to reach extremely high frequency levels of 300 GHz or even terahertz ranges. To support these new applications, 6G must simultaneously deliver high reliability, low latency and high data rates (Saad et al., 2019). The enabling technology will be Terahertz communications, satellite communications and AI.

Experts consulted in the development of this report forecast that emerging IoT cases that use 6G may include: Cross reality (XR) services composed of VR, AR and mixed reality; telesurgery; tactile internet; brain–computer interfaces; flying vehicles; and automated driving. Using satellite 6G to complement terrestrial IoT networks could also provide more comprehensive coverage for all of Australia, and thus support smart agriculture, utilities and transportation in RRR areas.

It is unlikely that 6G will be standardised and deployed before 2030. There are opportunities for the Australian Government and industry groups to participate in international discussions about 6G over the next decade and to prepare for future national deployment and preparedness.

4.3.5 Connectivity in rural and regional areas

Connectivity is a critical leveller to overcome the urban–regional digital divide. However, it is limited by commerciality and market forces. Coverage, quality, data availability, cost and choice of providers for connectivity are likely to be significant factors in the uptake of IoT applications in RRR areas, such as for agriculture and resource management. Emerging connectivity options should be used to supplement existing wireless communications, which may not be sufficient to provide good connectivity for the IoT in RRR areas. A 2018 CSIRO survey of 1,000 producers across 17 industries found that mobile coverage across their farms was commonly poor, with only 34 percent having full coverage and 43 percent having little or no coverage (Zhang et al., 2018). The report noted that 'existing telecommunications infrastructure may impose significant constraints to the potential utilisation of agricultural data technologies' (Zhang et al., 2018, p. 38).

Ongoing government initiatives to support improved mobile coverage and competition in RRR areas are encouraging. They include the Mobile Black Spot Program, which is supported by co-contributions from state and local governments, mobile network operators, businesses and local communities. As of October 2019, 748 base stations had been activated across Australia (Department of Infrastructure, Transport, Regional Development and Communications, 2020b). Fifty-three million dollars will also be invested to support investments by the telecommunications sector to build telecommunications infrastructure as part of the Regional Connectivity Program, which is part of the Australian Government's $220 million Stronger Regional Digital Connectivity Package (Department of Infrastructure, Transport, Regional Development and Communications, 2020c). In addition, the Universal Service Guarantee aims to provide all Australians with access to broadband and voice services, regardless of location, using NBN fixed line, fixed wireless and satellite. It will continue to use Telstra's existing copper and wireless networks in rural and remote Australia for the provision of voice services in NBN fixed wireless and satellite areas (Department of Infrastructure, Transport, Regional Development and Communications, 2020d).

In addition, connectivity will be an important factor in improving road safety and emergency management in RRR areas. While Australia's mobile footprint includes over 99 percent of the population, only one-third of the total landmass has mobile coverage (Infrastructure Australia, 2019). The Australian landscape has significant distances *between* populated areas, which can create barriers for systems which may need consistent and uninterrupted connectivity. For example, in consultation, the Austroads representative noted that emergency services struggle to locate road incidents in rural areas. There would be substantial benefits from improved connectivity for emergency management in RRR areas, with limited mobile coverage currently impacting on the ability of emergency services to locate incident sites. As CAVs are deployed over the next 10 years, ongoing research on how these can be integrated to enhance road safety and emergency management would also be beneficial.

Emerging options for low-power and long-range connectivity, such as Telstra's NB-IoT and Cat-M1 networks and the use of LPWAN networks, may be more appropriate for IoT applications. For example, Australian company mOOvement enables famers to build their own private long range (LoRa) network for IoT GPS ear tags and general sensor data collection (MOOvement, 2020). Mesh networks have also been considered, where relay nodes could be set up across existing infrastructure to extend connectivity to sensors in a wide area network (Tuffley, 2019).

Delay-disruption tolerant networking with remote sensors is another emerging alternative for agricultural applications in RRR areas. Using short-range distance communications, farmers in vehicles ('the collector') regularly collect data from sensors located at remote sites. Data can then be autonomously transferred into a data server located at a home base once the collector returns. While delivery of data is not real-time, as it is physically linked to the movement of the collector, early research using vehicles to collect data has demonstrated sufficient time-granularity for agricultural use cases, with near 100 percent delivery of data from sensor to home database (Ochiai et al., 2011).

Emerging satellite technologies via direct satellite upload connectivity are expected to provide alternative solutions to terrestrial wireless and commercial wireless options, with advancements in the next decade poised to make these technologies cheaper and more accessible. This is being explored by Australian companies such as Fleet Space Technologies and Myriota. Wi-Fi hotspots are also increasingly being used with satellite backhaul to provide localised connectivity in remote regions (e.g. for a single household or business). This set-up could be used in emergency situations where wide coverage is not required (Internet Society, 2019). Satellite technologies are discussed in Appendix B.10 in more detail.

The Australian Government should continue to assess infrastructure and connectivity requirements over the next decade. Further research is likely to be needed to explore the issues around connectivity, access and uptake of IoT technologies in RRR areas. In addition, community engagement and education on potential IoT use cases, as well as targeted digital capacity-building and skills programs are likely to encourage uptake and support economic development in RRR areas.

4.4 Environment and sustainability

Competition and innovation in the IoT industry has driven down cost, enabling the production of cheaper, miniaturised and low-powered devices and sensors. Discourse on IoT and sustainability has focused on aspirational goals regarding efficiency gains in resource consumption. However, this downplays the significant environmental impacts, particularly as deployment increases in cities and regions. Impacts need to be considered not only in relation to hardware (e.g. smart devices, sensors, data storage and transmission, and computation infrastructure) but also in relation to software, AI and machine learning. This is because these technologies will also shape individual and collective behaviour, institutions and policies, which may also create unintended negative environmental impacts. An example of this is the issue of potential 'rebound effects' which is discussed in section 4.4.1.1. Attention needs to be directed towards a more sustainable urban form of IoT deployment, which meets current and future expectations for sustainability.

4.4.1 Future energy consumption

The communications infrastructure underpinning the internet and connected devices, alongside data centres and servers that manage information flow, currently consumer two to five percent of electricity supply in countries such as Australia (Castellazzi et al., 2017; Jones, 2018; Morley et al., 2018). It is likely that devices connected to the IoT, will, on average, consume less energy than their internet counterparts, but this will be offset, to a degree, because there will many more of them. Similarly, the IoT communications infrastructure will typically carry less data than the internet, but it will need to communicate with more devices than the conventional internet and these devices will be spread more widely. If current predictions of the size and ubiquity of the IoT are correct, it is conceivable that IoT could consumer between one to five percent of the world's electricity by 2050. Further information on how the IoT may consume energy is discussed in Appendix B.11.

4.4.1.1 Rebound effects and increased consumption

Most industry and policy reports assume that the IoT will simply improve household management of energy consumption overall where more efficient resource use will result in a net reduction in overall consumption. However, studies have shown that the IoT has enhanced comfort, convenience, security and entertainment in ways likely to require *increased* energy consumption. This is known as a 'rebound effect' (Shove, 2003). Several studies conducted with Australian householders demonstrated that smart homes and devices often increased energy consumption (Hargreaves and Wilson, 2017; Nicholls et al., 2017; Roepke et al., 2010; Shove and Walker, 2014; Strengers and Nicholls, 2017). As a result, current estimates of the energy-saving benefits of IoT devices may overestimate the opportunity for energy reduction and/or load shifting. These issues are often downplayed in smart city or IoT literature on sustainability.

Examples of rebound effects are as follows:

- Smart parking or traffic control may reduce energy use and greenhouse gas emissions for individual car trips, but improved travel and parking conditions might decrease willingness to walk or cycle (Foth, 2018a) and encourage more car trips overall, leading to a total increase in energy use and emissions (Wang and Moriarty, 2018).
- Smart thermostats promise significant energy savings; however, over 30 percent of homes showed increased energy consumption after installation (Nest Labs, 2015). This may be due to increased usage time of heating and cooling appliances because the technology enabled users to pre-warm or pre-cool houses remotely before arriving home.
- Technologies that reduce the need for consumers to actively conserve energy can have carry over effects – diminishing energy management awareness and practices. For example, young adults moving out of a family home in which automation managed their energy use for them (via sensor lighting, smart thermostat, automated windows and shading) may struggle to manage energy use in a less technologically advanced home.

4.4.1.2 Impacts of manufacturing IoT devices

The environmental and sustainability impacts of manufacturing IoT devices are considerable. IoT devices require a significant amount of raw natural resources, including metals such as copper for electrical components and cobalt for lithium-ion batteries. Significant mining of minerals occurs in regions, such as Sub-Saharan Africa, which have little or no legislation or enforcement of social and environmental protections (Frankel, 2016). The mining sector in such regions has a track record of contaminating water and soil with heavy metals and hazardous substances and causing air pollution, for example with sulphur dioxide (Mwaanga et al., 2019). This affects the suitability of the habitat for flora and fauna, as well as posing a risk to human health. While investment in the mining sector has reduced environmental contamination through the modernisation of extraction and processing facilities (OECD Global Forum on International Investment, 2002), the demand for these raw materials continues to rise, increasing the risk of contamination and thus environmental degradation (Arrobas et al., 2017; Bleischwitz, 2014).

4.4.1.3 Lock-in, planned obsolescence and virtual wear-out

The demand for raw materials is at risk of multiplying if the service life of IoT devices is not maximised. Halving the lifespan of an IoT-enabled object can double the consumption of raw resources. For example, in smart cities and regions, while street assets and urban infrastructure objects are traditionally built from robust materials, their augmentation with IoT capabilities through retrofitting is costly and can pose technical compatibility issues. Upgrading this infrastructure so that it is compatible with the IoT then requires the complete replacement and disposal of otherwise functional infrastructure. This new IoT-enabled infrastructure is also at risk of requiring replacement before the end of the possible lifetime of its components. For example, hardware that no longer provides the latest data sensing capabilities or data transmission protocols is considered to be worn out virtually despite still being physically functional; it may need to be completely replaced. The smart city has therefore been considered as operating in a perpetual beta stage (Fredericks et al., 2019).

A number of factors could lead to high turnover of devices and the inefficient use of the resources needed to manufacture them:

- attempting to break out of vendor lock-in (Anastasiu et al., 2020; H. Robinson et al., 2013)
- incompatibility issues between hardware and software due to short innovation cycles, leading to virtual wear-out of infrastructure before physical wear-out (Hilty et al., 2004)
- planned obsolescence by IoT manufacturers, meaning that newer, more desirable products are released on short cycles and that products are not made to be durable, long-lasting or repairable (Wilson, 2019).

4.4.1.4 E-waste, disposal and recycling

The issue of e-waste is already a significant problem. The United Nation's Global E-waste Monitor noted that the world generated 53.6 million metric tons of e-waste in 2019, estimating that the amount of e-waste will exceed 74 million metric tons in 2030 (Forti et al., 2020). There are two factors that may lead to an increase in e-waste from the IoT: products and sensors that previously had no computational power are increasingly being transformed into devices with computational power, and device lifecycles have also been shortened (Higgenbotham, 2018).

The improper disposal or accidental damage of IoT devices can cause environmental contamination with toxic substances. These devices are difficult to recycle because they include a mixture of small recyclable and non-recyclable parts (City of Melbourne, 2016; Intouch Magazine, 2019). In addition, the proper recycling facilities are often not available, so the devices contribute to the growth of international e-waste sites. While new recycling and resource extraction methods are being trialled for IoT and other digital devices (Voutsinos, 2018), the cross-contamination of e-waste and other types of waste continues to be environmentally harmful (Koehler and Erdmann, 2004). Careful approaches to the management of e-waste will be needed moving forward.

4.5 Niche areas to develop the Australian IoT industry

The Australian Computer Society and PwC analysed opportunities to grow the IoT industry (PwC and Australian Computer Society, 2018). ACOLA also consulted widely with national and international experts in the field, many of whom have a deep understanding of the Australian market. Consulted stakeholders recognised that an IoT industry in Australia should build on existing expertise in specific sectors or develop niche solutions in the IoT stack. Agriculture, resource management, environmental monitoring and health were all considered to be areas where Australia had global scale or expertise. While overseas players lead in the IoT hardware market,[30] industry could consider developments in software and middleware, such as software for IoT-based health management or satellite-guided mining. Reducing our reliance on buying end-to-end components from countries that may have lower security and privacy standards than Australia would also be beneficial.

[30] There will be exceptions to this general rule. For example, Australian companies Fleet Technologies and Myriota are among global leaders in satellite IoT hardware development. These companies also have global aspirations and in some cases are on the way to achieving those on the back of R&D in the Australian market.

IoT initiatives in smart cities and regions are also an area for potential growth, such as solutions to make sense of mass-data collection in applied contexts. A state government noted in consultation that a challenge was exploring the value that could be gained from separate datasets gained from a number of IoT initiatives. There is therefore potential for start-ups or incumbents to develop models to better understand how different datasets can be used to enhance government service delivery. These applications would require robust, efficient and secure mechanisms for storing, transmitting and analysing data in real-time, and for providing application-specific information. The experience, knowledge, technologies and skills gained through this process could be generalised towards other IoT solutions. To maintain a competitive innovation advantage, industrial and academic R&D incentives for generalisable application developments might play an enabling role here. Specific opportunities for local start-ups and incumbents to develop tailored niche solutions were noted in the following areas.

4.5.1 Cloud services

The cloud services market is served by large multinationals including Amazon, Microsoft, IBM and Google, with some network providers such as Vodafone and Telstra providing cloud services within their integrated vertical solutions. The cloud market will be a difficult market for Australian players to compete in (PwC and Australian Computer Society, 2018). Industry start-ups should therefore consider cooperating with major players to provide specific supplementary services or solutions that can provide add-ons to complement existing services. Larger providers could seek to offer specific niche solutions for industry verticals where cloud services are already integrated in the existing integrated solutions.

4.5.2 Enablement platforms

Platform solutions for end users is another area for potential growth, with the platform market still considered relatively immature. This market is expected to remain competitive and fragmented in the near term (PwC and Australian Computer Society, 2018). It is expected that this area of the IoT value chain will be bundled with up-stream (such as applications) and down-stream (such as connectivity and cloud storage options) offerings for customers (PwC and Australian Computer Society, 2018). It is forecast that offerings will become integrated ecosystems where customers will be able to access end-to-end solutions, rather than a piecemeal system or building one from the ground up. Australian companies should establish niche applications that can be integrated with existing platform solutions, so it will be important to form the right strategic partnerships.

4.5.3 Connectivity

There may also be niche areas for growth in the connectivity and telecommunications spaces. For example, we have seen the roll out of a range of connectivity options across the different networks, including Sigfox (licensed by Thinxtra), NNNCo, Meshed and Definium, all providing alternative options to larger incumbents.

Australian companies such as Fleet Space Technologies and Myriota show promise, leading Australian efforts to deploy satellite connectivity options, which may provide more choice for connectivity in RRR areas. The Australian Government's Regional Connectivity Program also aims to promote private sector involvement with government subsidies.

With available unlicensed spectrum, there are opportunities for new entrants, including overseas players and local start-ups, to enter this market. Local start-ups may be able to carve out a niche area, for example, by providing connectivity options to RRR areas or collaboration with players in the agriculture or health sectors, given Australia's expertise in these sectors. There may also be opportunities for local start-ups to create 'localised solutions for the edge and other adjacent solutions' (PwC and Australian Computer Society, 2018, p. 58).

4.6 Opportunities and challenges

4.6.1 Regulatory sandboxes

The Australian Human Rights Commission has suggested the use of regulatory sandboxes, where companies can test products and services for a period of time under the authority of a regulator, before obtaining the usual permit or licence. Currently, there are at least 31 operational regulatory sandboxes globally (UNSGSA FinTech Working Group and CCAF, 2019). The use of sandboxes would enable manufacturers and service providers to be exempt from legal liability, as well as providing access to expert advice and feedback on their regulatory responsibilities prior to going to market (Australian Human Rights Commission, 2018b).

This approach could draw on existing work and learnings from the Australian Securities and Investments Commission's regulatory sandbox framework which enables fintech products or services to be tested without obtaining a financial services or credit licence for 24 months. The Australian approach was modelled on the UK Financial Conduct Authority's sandbox initiative, which has been successful in demonstrating that regulators can 'play an active and positive role in encouraging innovation', challenging the view that regulation is a barrier to innovation (Deloitte LLP, 2018). The Financial Conduct Authority's review of this initiative in 2019 found that 80 percent of firms successfully tested in the sandbox are still in operation (Financial Conduct Authority, 2019). It has since launched a 'global sandbox' to enable start-ups to navigate cross-border regulatory environments to participate in a global market (Financial Conduct Authority, 2019).

Positive steps that could be modelled in Australia to enhance existing measures include publication of a 'Lessons learnt' report following the establishment of the program, as well as establishing bilateral agreements to facilitate sandboxes with key markets. In addition, there is the opportunity to use the sandbox initiative to provide greater consumer protection and recognition to social and ethical issues such as accessibility and bias, which could be assessed before a new product or service enters the market.

4.6.2 Interoperability

The interoperability of IoT technologies can be achieved by the development of a universally accepted standard, such as the TCP/IP (Transmission Control Protocol/Internet Protocol) standard in the computer network. The economic benefits from better interoperability are likely to be significant. While this is difficult to measure, to provide some context, McKinsey has estimated that interoperability is required for 40–60 percent of the potential benefits of the IoT to be realised (noting their 2015 estimate that IoT will have a total potential economic impact of $3.9–$11.1 trillion a year by 2025) (Manyika et al., 2015). Future interoperability will provide a counterpoint to today's IoT technology, which typically only interoperates well within a silo from each manufacturer.

However, the development of interoperability is challenging and requires collaborative efforts from academia and industry. It is predicted that several interfaces between big IoT platforms will be developed to improve interoperability in the next two to five years, with international standards being refined over the next decade. In addition, interoperability will increasingly be needed at human semantic levels in addition to current technical levels so that consistency of knowledge derived from raw data within the IoT can be checked at human-relevant levels of interaction.

4.6.3 Interoperability challenges for the mobility sector

Interoperability has been raised as a key challenge for the mobility sector, given that most vehicles are manufactured overseas, with competing technologies and protocols being preferred by different manufacturers.[31] Australian governments and independent bodies such as Austroads and the National Transport Commission should ensure harmonisation across all state and territory jurisdictions to ensure that CAVs can operate across long distances and jurisdictional borders. A useful model to follow is the establishment of common standards for electronic toll collections, as this has facilitated the use of a single in-vehicle tag for all tolled roads in Australia.

4.6.4 Network infrastructure considerations

There is a clear role for the Australian Government to play in considering the infrastructure and connectivity options necessary to facilitate access to the IoT in RRR areas over the next decade. Initiatives such as the NBN rollout in regional areas, the Universal Service Guarantee, Mobile Black Spot

[31] See discussion in Chapter 2, section 2.2.2.2.

Program and the Regional Connectivity Program are encouraging, demonstrating an existing commitment to providing connectivity regardless of location. However, further research and ongoing evaluation of these programs, as well as the assessment of emerging technologies such as LEO satellites are recommended. The use of these technologies to enable regional IoT applications in agriculture and resource management are likely to provide long-term economic benefits in RRR communities over the next decade.

4.6.5 Adopting a holistic ecology approach to environmental impacts

Most IoT investment in smart cities and regions has been driven by a technocentric approach. While this may produce efficiency gains, genuine sustainability requires a holistic ecology perspective (Foth, 2018; Yigitcanlar et al., 2019). Sawyer noted that:

> *"Information and communications technology, data and networks have an important place in our shared urban future. But this future will be determined by our attitudes toward these technologies. We need to make sure that instead of being short-term gimmicks to be thrown away when their novelty wears off, they are thoughtfully designed, and that they put the needs of citizens and environments first"* (Sawyer, 2018).

Various commentators have called for citizens to be put first in response to the release of Australia's Smart Cities Plan (Foth, 2016), as well as in response to the technocentric deployment of smart cities (Foth, 2018; Foth et al., 2016; Mattern, 2019). The statement above puts both citizens and the environment first, and rightly questions the concept of 'human exceptionalism'. This may require a new paradigm that reconceives the human relationship with nature and planetary health in the design of smart cities and regions. This has been described as 'decentering the human' in the design of collaborative cities (Forlano, 2016). Questioning humans as the exclusive inhabitants of the built environment allows designers and policy-makers to consider a more inclusive and encompassing worldview. This post-anthropocentric perspective entails a re-think of human-centred design and architecture and aims to build smart cities and regions from a more than human perspective and using world-centric design methods (Foth, 2017; Luusua et al., 2017; Smith et al., 2017). These considerations should be embedded in the larger debate on the ethics and responsibilities of the design sector, urban planning and the digital technology industries (Monteiro, 2019).

4.6.6 Energy management

Various strategies for energy management through IoT-enabled devices and automation have been proposed, both in Australia and internationally (CSIRO, 2013; Energy Networks Australia and CSIRO, 2017; National Grid, 2016), which may help address unintended impacts such as rebound effects. Recommendations for future strategies for Australia are that:

- energy efficiency strategies should not rely solely on technological change but should be complemented by sufficiency strategies[32]
- IoT deployments should be accompanied by education, awareness and behavioural change strategies on the consumer side
- energy efficiency evaluations should account for how technologies will be likely to be used in practice, and shift focus from individual products to networks (Gossart, 2015).

Strong and ongoing community engagement will be needed to maximise the benefits of IoT-enabled energy. Following an extensive international literature review and research with Australian households and energy sector stakeholders, community approaches could consider:

- changing terminology for people from 'customers' and 'consumers' to 'partners', 'flexible opportunists', 'carers' and other meaningful roles that better reflect how people engage with energy in their daily lives
- engaging people through issues, concerns and everyday practices that already interest them (such as caring for their children or pets)
- recognising ways that people value energy, extending beyond its role as a market commodity (e.g. as a community asset, shared responsibility or common good)
- communicate with the public in an engaging manner, as suggested in the Future Grid Engagement Strategy (Strengers et al., 2019), such as through the use of activity vouchers to incentivise people to leave homes during periods of peak electricity demand, or free or discounted pet heating and cooling technologies for heat vulnerable pets as an alternative to air conditioning and heating.

Governments and industry could consider measures which seek to encourage lower-energy digital lifestyles as new IoT devices are integrated into society. This will require consideration of health, education, defence and ICT (national broadband) factors in energy consumption initiatives (Royston et al., 2018).

[32] 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.

4.6.7 Transitioning to a distributed energy system

Given Australia's relatively high-cost electricity market, smart grid transformations are likely to transition towards a distributed energy system, providing more choice for consumers and reducing cost. It will be important to establish standards to define and regulate this 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. The Energy Security Board has been tasked by the Council of Australian Governments Energy Council to develop advice on a long-term, fit-for-purpose market framework that could apply from mid-2020's. (COAG Energy Council, 2020).

4.6.8 Incentivising sustainable and holistic approaches in IoT design and development

Environmental concerns should be considered as an integral component in the manufacturing of devices. Incentivising industry to take holistic or sustainable design approaches, in the development and manufacture of IoT products over the next decade will be important. Circular economy strategies where value is retained as much as possible from resources and materials used, including the mining of potential e-waste from the IoT, should be considered an important source of secondary raw materials (Forti et al., 2020). It has been estimated that a five percent improvement in material efficiency would represent a $24 billion increase to GDP in Australia, creating 9.2 jobs for every 100,000 tonnes of waste recycled (Boxall et al., 2019). CSIRO notes that while there are opportunities to reinvigorate the Australian manufacturing industry to remanufacture materials from secondary sources, R&D in waste innovation and circular economy is currently largely fragmented, and linkages and collaborations between industry, government and other stakeholders will be required to build critical mass (Boxall et al., 2019).

4.6.9 Further research into environmental impacts of IoT

In addition, further research is required to understand the environmental impact of the projected growth of IoT devices over the next decade. Vendor lock-in, virtual wear out and planned obsolescence may increase the volume of e-waste exponentially. Opportunities to mitigate these risks, such as encouraging sustainable design, extending the lifecycle or improving the usability of existing devices would be beneficial for industry to consider (Zallio and Berry, 2017). Upgrades, unobtrusive plug-ins and smart add-ons could increase the life expectancy of existing devices and enable users of various ability to use them for longer periods. For example, Apple Genius customer support technicians are provided with repurposed iPods or iPhones to use. These devices have been upgraded with bigger protective case, embedded with a long-lasting battery, a credit card terminal, a radio-frequency identification (RFID) sensor and simple software to manage sales, calendar and tasks (Zallio and Berry, 2017).

4.6.10 Australian satellite and space technology to support the IoT

Significant opportunities exist for Australia to adopt satellite and space technology, including stratospheric drones and balloons to enable internet connectivity for over 70 percent of the landmass not serviced by terrestrial fixed and wireless networks.

Opportunities:

- Infrastructure to support automation, robotics and IoT applications in agriculture, mining, energy and long-distance transport.
- Communication networks in regional Australia including land, airspace or marine regions.
- Establishment of ground infrastructure for launch and retrieval sites for high-altitude pseudo satellites (HAPS), stratospheric drones and stratospheric balloons servicing the Asia-Pacific region.
- Development of sovereign industrial capability and commercial expertise in nanosatellite and small satellite constellations, as well as IoT services for RRR areas
- Development of manufacturing capability for small satellites.
- Establishment of access to space launch sites and sovereign small rocket capability for launch of small satellites for polar and equatorial orbits.
- In the next decade, telecommunications tentatively characterised as 6G, could be powered by satellite, which will enable ultrafast, reliable and low latency connectivity for AI-based collaborative processing of big data which could optimise systems such as transportation networks, smart grids, financial market monitoring and healthcare systems.

Practical measures to support implementation:

- Completion of the Geoscience Australia-led augmentation system to provide 10 cm positioning accuracy across our land, marine and airspaces and precise positioning to the accuracy of 3 cm in our cities, using additional correction to the GPS signals with the mobile phone network. This infrastructure provides a critical platform for automation, the IoT and smart city development (Geoscience Australia, 2019).
- ACMA to continue to consider spectrum allocation that supports terrestrial and space-based communication infrastructure.
- The Civil Aviation Safety Authority and the Australian Space Agency[33] to continue to collaborate on the legal and regulatory framework above and below 20 km for access to the stratosphere and space.
- Progress the Australian Space Agency 10-year strategy 'Advance Space' (Australian Government and Australian Space Agency, 2019) to foster international collaboration, increase national capability, promote responsible regulation risk management, and culture and inspire and build a future workforce.

Challenges:

- Spectrum allocation and sharing for terrestrial wireless networks and space-based infrastructure.
- Global competition in establishing the space-based internet and network infrastructure is well advanced and attracting significant infrastructure. Australia has yet to establish a globally competitive position in this area. There is the risk that Australia is unable to develop its own sovereign capabilities in this area, if it only uses imported technology and services.

[33] The Australian Space Agency was established by the Australian Government in July 2018 to coordinate civil space matters across government and support the growth and transformation of Australia's space industries. There are likely to be parallels between the agency's work and future developments in the satellite telecommunications sector to support IoT deployments.

CHAPTER 5
SOCIAL AND COMMUNITY CONSIDERATIONS

Chapter overview

Short-term

- Across Australia and internationally, communities are at relatively early stages in their knowledge about and engagement with the IoT.
- Early outreach to the community would be helpful to promote better understanding of the value of IoT technologies, such as the rollout of smart city and region initiatives, as well as driving interest to adopt appropriate technologies.
- Understanding the social and community considerations of the IoT should be a priority for IoT development, particularly for vulnerable populations, including people with disabilities and the elderly. Design, policy and research should be conducted in the next three to five years and will require a coordinated approach.
- Community participation in and engagement with IoT plans, development and policy will be imperative, with appropriate support and resourcing required. Community will need to be consistently engaged and coordinated across each level of government.

Medium-term

- The IoT will initially be distributed unevenly across communities and users, and this will likely expose and exacerbate existing socioeconomic inequalities and disadvantage. To avoid further perpetuating inequalities, IoT services should be explicitly designed to reflect the wishes and needs of diverse groups of citizens.

Long-term

- In the future, it will be important to consider the design and planning of our smart cities and regions from a holistic ecology approach, reconceiving our relationships with nature and planetary health. Designers and policy-makers should strive to have an inclusive and encompassing worldview that considers people as part of broader ecosystems of living things, rather than as the exclusive inhabitants of the built environment. These considerations should be embedded in the larger debate around the ethics and responsibilities of the design, urban planning and digital technology sectors (Monteiro, 2019).

5.1 Introduction

The IoT is bringing into the foreground how people both shape and are shaped by environments and technologies. While it is likely to be too early to identify a significant trend in the way the IoT will have an impact on social interaction and relationships, it will inevitably change how people interact with their environments and each other. A key consideration is devoting attention to how people will use the personal data generated by IoT technologies as part of their everyday lives and social interactions, and how third parties will seek to exploit these data for commercial or political ends.

5.2 IoT and the community

Worldwide, communities are at relatively early stages in their engagement with the IoT. Rather than seeing the IoT as a force that will act on communities in cities, regions and rural areas, research has shown that it is more accurate and productive to pay attention to the two-way relationships between technology and communities (Bunz and Meikle, 2018). As the many examples across this report show, the way communities and users adopt, adapt and imagine novel technology is a crucial part of the long process of technology invention, implementation and diffusion. Already, there are a range of changes underway in cities, with adoption and deployment of the IoT and associated technologies. However, researchers have noted that while the social *imaginaries* of smart cities have received wide attention in public and policy discussions, the realities of living in the 'actually existing' smart city have yet to be fully researched (Shelton et al., 2014).

Critical urban studies research has shown that smart city initiatives and partnerships present numerous potential tensions (Caprotti and Cowley, 2018). The smart cities vision partially relies on connections between different spheres of urban management, which can lead to difficulties such as:

- corporate actors focusing smart city technologies on wealthy cities or areas with the capacity to pay for their services, to the exclusion of less socioeconomically advantaged areas

- public sector services lacking resources and technological expertise compared with those enjoyed by the corporate smart city providers with which they attempt to partner (Taylor Buck and While, 2015)
- the needs of specific areas being ignored for a focus on developing universal solutions
- increasing moves towards splintering and disaggregation of services, such as privatisation, negatively impacting users or leaving out population groups.

Households play a decisive role in how social relations among people and their environments change with technology. They are therefore a crucial place to look to understand the social implications of the IoT and a key focus for emerging research.

5.3 New challenges for users

User experience of the internet has evolved over the years and has become increasingly complex. The IoT is part of the development of Web 4.0, which has enabled connections between the internet and other users anytime and anywhere, as well as the personalisation of services based on the continuous stream of data (Deursen et al., 2019). The IoT presents four new challenges for users compared to previous uses of the Web (Deursen et al., 2019):

- the ubiquity of devices increases the *amount of data* generated
- as devices are often unnoticed and can make autonomous decisions, the result is *less autonomy* from a user perspective
- data collection is much less visible and the resulting consequences (often determined by organisations and devices that are removed from the user) are difficult to predict so there is *less visibility and more ambiguity*
- *security and privacy risks are magnified*, given that security measures are varied, and the amount and diversity of data are much more granular, detailing habit profiles, demographics and wellbeing.

These four features demonstrate how the IoT will bring new challenges for users, but at this stage, it is unclear how this will impact on different individuals (Deursen et al., 2019).

5.4 Social inequality

Income differences and educational levels have been found to impact on attitudes around the use of IoT devices. Those with higher levels of education and higher incomes have more positive attitudes towards IoT devices and are more likely to be the first to buy them. This means that they are also the first to develop the skills required to engage in diverse uses of the IoT (Deursen et al., 2019). Similar conclusions occur across age, with younger people tending to have the most material IoT access and a higher level of IoT skills (Deursen et al., 2019).

Researchers interested in human rights and social justice issues argue that the IoT is implicated in a number of 'data harms' (Redden and Brand, 2019), including punitive or exploitative uses of 'dataveillance': the watching of people using data generated about them (Best, 2010; Sadowski, 2019; Sadowski and Pasquale, 2015). These harms include becoming the subject of hidden surveillance, identity theft and denial of opportunities such as access to credit, social services and insurance (Maras and Wandt, 2019; Zoonen, 2016).

The potential for the algorithmic decision-making processes undertaken by IoT technologies to be biased, exacerbating social inequalities and social marginalisation, has also been identified (Lindley et al., 2019). Social researchers have noted that dataveillance disproportionately affects already marginalised and disempowered social groups, frequently exacerbating poverty, racism and sexism (Eubanks, 2018; Noble, 2018; O'Neil, 2016). IoT systems can potentially contribute to these processes. In some parts of Australia, for example, smart city technologies have been implemented in ways that are directed at making the activities of Indigenous populations more visible, perpetuating racism and socioeconomic disadvantage (O'Malley and Smith, 2019). Further information on algorithmic decision making can be found in Appendix D.4.5.

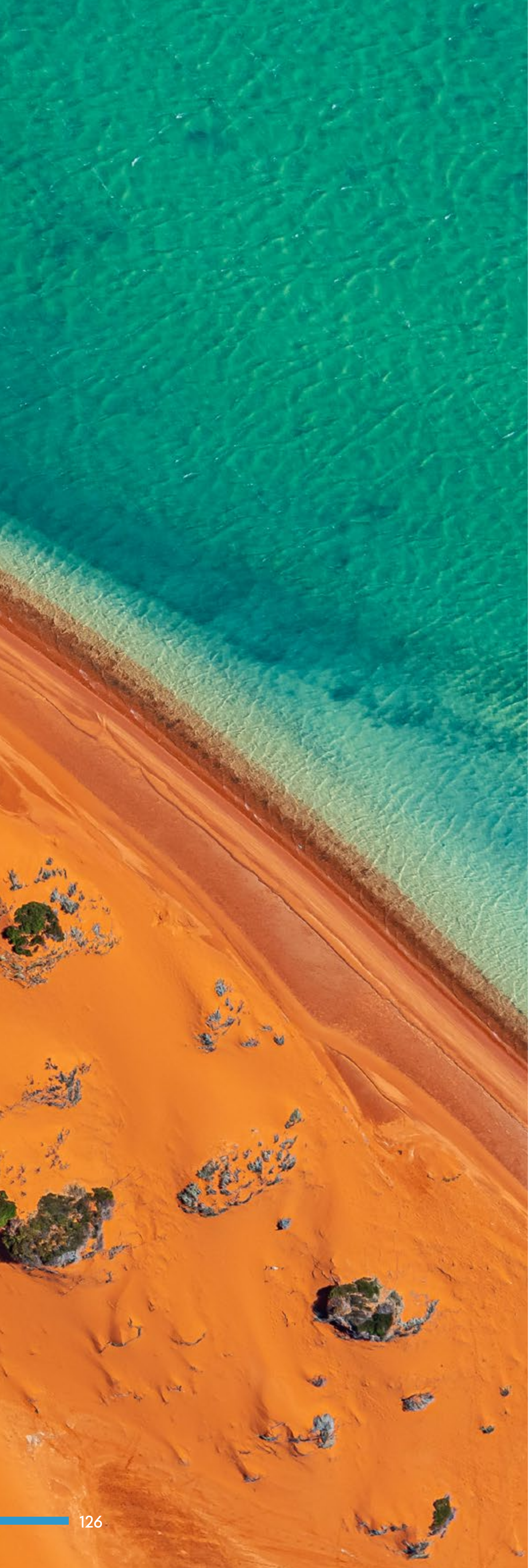
Researchers analysing the enactments of smart cities have shown that initiatives and partnerships involve numerous potential tensions (Caprotti and Cowley, 2018; Karvonen et al., 2019; Taylor Buck and While, 2015). These include the partial reliance of the smart cities vision on connections between different spheres of urban management and service provision, in the context of increasing moves towards the splintering and disaggregation of these services, such as privatisation. Another tension emerges from the tendency of corporate actors offering smart city technologies to focus on wealthy cities or areas in cities with the capacity to pay for their services, to the exclusion of less socioeconomically advantaged areas. Further, the contextual needs of specific areas require attention in service provision, but these are often ignored for a focus on developing universal solutions (Caprotti and Cowley, 2018; Karvonen et al., 2019; Taylor Buck and While, 2015).

5.5 Psychological impacts of the IoT and impacts on vulnerable populations

It is important to consider how the IoT may impact on community members in novel ways, such as psychological impacts or impacts on vulnerable members of the population including women, children or those from ethnic minorities. These issues are discussed in more detail in Appendix E.1.

5.6 IoT and Indigenous populations

The IoT presents several concerns from an Indigenous perspective, including issues related to cultural need, community infrastructure, environmental concerns and Indigenous sovereignty. It is important to note that these concerns extend beyond approaching communities with cultural sensitivity to the fact that Indigenous peoples position themselves in a custodial role in relation to the environment, the land and living things. The impacts of the IoT also have the potential to exacerbate pre-existing issues and grievances in Indigenous communities in some cases. While the presence, uptake, interest and impact of emerging technologies in Aboriginal communities have received research attention (Rennie et al., 2019; Thomas et al., 2019), no research has been conducted specifically on their IoT use. Organisations such as the Centre for Appropriate Technology Limited, a not-for-profit Aboriginal and Torres Strait Island organisation, support community engagement and uptake of technology. Further research on the specific impact of the IoT on Indigenous people and communities would be beneficial as this technology matures. In the development of this report, a number of key concerns were raised around the emergence of the IoT. These are outlined below.



5.6.1 Systems of knowledge: conceptual alignment of digital systems with ecosystems

The IoT presents a data-centric way of 'knowing' about the world. The rollout is expected to collect large amounts of information about the physical environment and is described as producing a 'digital ecosystem'. This framing bears very little resemblance to the ecosystem as Indigenous people understand it.

The IoT also opens the possibility for the living things (animals and plants) and physical aspects of the environment to interact and become responsive to each other, without the need for human intervention. This is in conflict with Indigenous understandings of the relationship between humans and their environment, according to their land-based, physical, seasonal and cultural systems of knowledge. For example, technologies used to generate knowledge about the distribution and use of resources may threaten existing Indigenous understandings of the physical landscape.

5.6.2 Sovereignty and self-determination

Data sovereignty for Indigenous people includes the ability to retain control over data, as well as the ability to undertake digitised collection and storage of traditional knowledge, cultures and languages. Many Indigenous communities are now finding ways to protect their data sovereignty using existing technologies. The IoT generates two key challenges to this:

- the proliferation of technological devices and data-collection practices which are *not chosen or controlled* by Indigenous peoples can be seen to challenge existing ideas about Indigenous sovereignty and self-determination

- increased data-gathering practices may increase the *feeling* of surveillance and control mechanisms over Indigenous populations.

5.6.3 Accessibility, digital literacy and marginalisation

Common to many rural and urban populations, the IoT presents some Indigenous communities with issues of:

- access: even though the IoT is a pervasive influence on social life, individuals and communities may be denied access because of problems related to their location and financial barriers
- digital marginalisation: individuals who live outside of communities that have IoT access or who choose to opt out of IoT technologies may be at risk of being increasingly marginalised, as living outside of a digitised society becomes increasingly difficult.

User acceptance is often perceived as the main barrier to economic growth. The idea of 'compliance' with an IoT framework or 'acceptance' of its practices, however, is a deeply threatening concept for many Indigenous communities, and the importance of this should not be understated. Bridging this gap should be approached with caution.

Gaining public trust involves engaging with communities, and for marginalised communities this may involve targeted support for minorities. Indigenous consultants have expressed the view that digital marginalisation should not be reduced to 'inadequate digital literacy', to be remedied with education. This can be interpreted as presuming to 'correct' or 'solve' a knowledge-based 'lack' in Indigenous communities.

Communities may also be resistant to welfare in the form of support programs designed to modify behaviour and up-skill individuals for participation in the economy, when past attempts to achieve similar goals have been unsuccessful and destructive.

5.6.4 Connections with the landscape

The encroachment of the IoT affects Indigenous communities' spiritual connection with the landscape. Some concerns relate to the sickness or death of the land. For example, removing parts of the land (i.e. extracting resources such as rare earth metals and sand for manufacturing and energy) threatens to displace spiritual connections. Indigenous communities are conscious that terrestrial sources of sand are almost exhausted, and growth in the IoT will demand more resource extraction. Similarly, waste must sometimes be stored for millennia in the land. Growth in the IoT increases the number of discarded devices and manufacturing produces toxic and sometimes radioactive waste. Plans for technological development often obscure how the landscape will absorb this waste.

5.7 Literacy and affordability

An individual's ability to participate fully in IoT technologies is dependent on characteristics such as digital literacy, financial situation, connectivity and data access. For example, the potential benefits of the IoT to enable an individual to manage their energy supply and consumption will be spread unevenly. This risk has parallels with the shift towards internet banking and the closure of regional bank branches and post offices, which has left rural and older Australians, who don't always have access to computers, the internet or digital skills, with limited capacity to do banking or pay bills (Australian Government, 2004).

ABS data indicates that about 20 percent of people aged 55–64 years and about 40 percent of those over 65 years do not use the internet; usage of the internet is significantly higher in cities than in RRR areas (Australian Bureau of Statistics, 2018). Of those who do use the internet in these age groups, it is likely that a significant proportion are not sufficiently 'tech-savvy' to use IoT devices for energy purposes. Planning and policy are typically delivered by digitally skilled professionals in urban areas and do not always take into account unintended and unforeseen impacts on regional, remote, older, low-income or digitally excluded citizens. Australian Government initiatives include: funding network partners of the Be Connected Program (which provides online resources and courses to support digital learning for seniors) to purchase digital devices and sim cards to loan to individuals so that they can access online services and stay connected during the COVID-19 pandemic (Minister for Families and Social Services, 2020); and the implementation of an online Digital Technology Hub to provide RRR communities with information on digital technologies and support connected and unconnected customers as part of the Regional Connectivity Program (Department of Infrastructure, Transport, Regional Development and Communications, 2020a).

In the energy sector there is a considerable emphasis on the widespread rollout of 'cost-reflective' electricity pricing (higher charges at peak times) and use of automation to shift appliance usage to lower price periods. While this might benefit the system as a whole, households without internet, time or digital skills may be financially disadvantaged during this transition as demonstrated in Case study 25.

Case study 25: IoT literacy and affordability – a trial in Australia

Automation and the IoT are often not as easy and useful as they are marketed to be. Researchers conducted a trial with 40 households in Victoria and South Australia, where participants were asked to self-install market-leading smart light bulbs and plugs. The bulbs and plugs would provide automation and smartphone app-mediated control of appliances (Nicholls et al., 2017). Key findings of this research included:

- a quarter of trial households were not sufficiently interested or digitally confident to attempt to install the devices
- a quarter of trial households tried to install the devices but could not get them working
- a quarter of households installed the devices but later abandoned use due to product failures they could not resolve, inconvenience or other reasons
- only a quarter of households installed the smart devices and were still using them three to six months later (not necessarily to manage energy use but for lifestyle improvements).

These results not only indicated the potential for significant technology waste, they also demonstrated feelings of confusion, inadequacy, frustration and exclusion among technology users. However, these negative experiences need to be balanced against potential benefits for those that successfully use these devices to manage energy use.

5.8 Building community trust and acceptance

The use and uptake of emerging technologies is 'dependent on a responsible regulatory system that encourages innovation and engenders confidence in its development' (Walsh et al., 2019, 6). Trust is established as a multi-layered concept, spanning:

- good user-centred, inclusive design (e.g. as accented by 'trust by design' and ethical design proponents)
- strong policy frameworks, with consumer, citizens and rights protections built in from the outset
- functioning competitive markets in which trust is a key goal and where consumer choice can be properly exercised
- genuine and ongoing community engagement in technology development (Baldini et al., 2016).

Communities can become distrustful of technology where it misleads or breaches trust of those who use it. Poor public trust in governments and corporations may prevent effective adoption and diminish benefits of emerging technologies (Walsh et al., 2019). Use and attitudes towards the IoT are also likely to be uneven and will depend on diverse criteria, such as education, age, income levels and ethnicity. There will also be specific considerations for vulnerable cohorts, such as people with a disability or the ill. Appendix E.2 provides more detail of some of impacts on specific populations

It is important that regulatory systems limit adverse outcomes and are seen to protect citizens. Measures must be designed transparently and show sensitivity to public attitudes. Adverse human rights implications, such as discrimination, implicit bias or undisclosed reasons can undermine trust, and may result in pre-emptive calls for regulation or limit uptake In Australia, executive bodies responsible for promoting and protecting human rights include: the Human Rights Commission, the Office of the Australian Information Commission, the ONDC, the Office of the eSafety Commissioner and the ACCC (Walsh et al., 2019).

Recent developments in Australia specifically pertaining to the development of the IoT include:

- The Australian Human Rights Commission's Human Rights and Technologies Issue Paper (2018) and Discussion Paper (2019) outlines some of the risks of emerging technologies, including safety and security issues for the IoT (Australian Human Rights Commission, 2018b; Australian Human Rights Commission, 2019).
- The Australian eSafety Commissioner has developed Safety by Design Principles to provide guidance to industry on assessing, reviewing and embedding user safety in online services, with a Framework of Guidance for industry use to follow (Australian eSafety Commissioner, 2019).
- The ACCC recognised interconnected devices as one of its Product Safety Priorities for 2019 and the importance of 'rais[ing] awareness and build[ing] capacity to address consumer safety hazards' (Australian Competition and Consumer Commission, 2019b).

The issue of trust is discussed in more depth in the ACOLA report *The effective and ethical deployment of artificial intelligence: An opportunity to improve our wellbeing* (Walsh et al., 2019): while this report relates specifically to AI, the considerations for the IoT and emerging technology are much the same. As with all emerging technologies, developing trust and acceptance will encourage more uniform uptake of IoT technologies across communities over the next decade.

5.8.1 Accessibility and inclusive design

The role of inclusive design in accommodating and involving those experiencing difference, disability or disadvantage has been discussed previously (Walsh et al., 2019). Incorporating inclusive design principles in the development of devices and relevant policies, which consider the characteristics and needs of a wide range of users, during conceptualisation rather than after development, can proactively address issues such as technology obsolescence or discontinuance, as well as enhancing social and cultural acceptance (Moon et al., 2019). For example, IoT wearables, and devices more broadly, can increase accessibility, independence and community participation for people with disabilities (Moon et al., 2019).

5.8.2 The value of public engagement

Due to the emerging nature of IoT technologies and smart cities, there is limited research in how to best educate the community to encourage uptake of the IoT. However, broader studies have been performed that indicate the importance of community engagement in the uptake and adoption of technology. Often engagement and education of the community comes after an initiative is mostly rolled out; however, this approach can undermine the power of a community. A clear starting point for gaining public trust is ensuring that the wider community is engaged in technology design, implementation and adoption. This could include engaging on the rollout of smart city and region initiatives, as well as driving interest to adopt relevant technologies. This could be facilitated through an online presence to express the potential value of the IoT or through joining other communities to express ideas.

For example, the Tasmanian Government and the Australian Government have contributed significantly to raising awareness of the LoRa LPWAN within the state, as part of the Launceston City Deal. This was done by undertaking training workshops, trials of wearables and agricultural sensors, and instigating the LoRa schools challenges (Australian Government and Regional Development and Communications, 2018). Further to this, the city is engaging with a range of stakeholders to determine the best ways to further promote the NBN and deliver programs to improve digital literacy (digital skills and capabilities) in the community.

Sharing knowledge and increasing exposure of IoT projects, particularly smart cities and regions, to targeted members of the community can help foster and accelerate community understanding of and interest in IoT deployment. A focus on sharing use cases is a dynamic and approachable way to communicate the objective of a project in a real-world setting.

In consultation, the Australian Communications Consumer Action Network raised the idea of regularly surveying Australian consumers across diverse social groups and interests to obtain information on what they are doing in relation to IoT technologies and what benefits and risks they perceive (perhaps on an annual basis), so that there is baseline research available to inform government and corporations.

Developing a living labs approach is one way to include the voices of diverse community groups in planning. This approach uses participatory design activities that encourage community participation in planning for the deployment of the IoT in a sector or region.

There are also opportunities for school curricula to be developed that engage students creatively and critically with topics and issues concerning the IoT and its futures. Developing soft skills at primary and secondary education levels will help broaden early awareness and understanding. Initiatives may also be used to increase engagement and knowledge in students' families and the wider community as a secondary effect. For example, the Australian Government's Digital Technologies Hub hosts online learning resources and services encourages learning and access teachers, students, school leaders and families (Department of Education, Skills and Employment and Education Services Australia, 2016).

Community engagement with the IoT can positively impact smart city and regional development in two ways, as outlined in the following sections.

5.8.2.1 Help build an equitable future

Researchers in critical urban studies have argued that there is a need to incorporate community engagement in future planning, in order to imagine a more socially equitable future for smart cities. A citizen-led approach that foregrounds the interests of socially and politically marginalised, disadvantaged or excluded groups is needed, to protect vulnerable citizens from an agenda oriented purely by corporate interests (Leontidou, 2015).

5.8.2.2 Findings can help to grow understanding of how communities will use the IoT in practice

Little is known about citizens' desires or aspirations for smart environments such as smart cities or smart homes, and more research is needed (Vanolo, 2016). Social researchers have called for smart city forecasting that incorporates a thorough understanding of how people respond to new technologies as part of their daily lives (Strengers et al., 2019). For example, in their project involving developing future-oriented scenarios, Strengers and colleagues found that people wanted to use smart energy systems to cater for the needs of their pets, a practice not previously considered in measuring the efficiencies of smart homes (Strengers et al., 2019).

5.9 Opportunities and challenges

To build a picture of citizen experience, research internationally has begun to highlight early adoption and usage of the IoT in areas such as:

- automated voice assistants and home technologies (popularised with Google Home and Amazon Alexa devices)
- smart home systems, offering control of doors, windows, electricity, entertainment, music and media systems
- sensor and data-based technologies in security systems but also emergent health, home, disability and aged care
- public and private transport, and other forms of mobility.

Public attention and research on IoT is limited in scope. At present, the evidence on how the IoT interacts with social change factors in the Australian context is still unclear. More research needs to be conducted on the social and cultural dimensions of IoT use across the broad range of potential domains of use in Australia, including farming, education, transport and industry, as well as across households and different population groups. This is required to fill current gaps in knowledge about how Australian consumers across these domains understand what is meant by the IoT, what benefits they are gaining from these technologies, what risks and harms might be affecting their use or avoidance of IoT technologies, and what developments and improvements they would like to see in the IoT to better suit their needs.

Understanding the social and community considerations of the IoT should be a priority for IoT development and design, policy and research in the next three to five years, and this will require a coordinated approach. Community participation in and engagement with IoT plans, development and policy will be imperative, and there is a need for appropriate support for and resourcing of this engagement. Communities will need to be consistently engaged and coordinated across each level of government.

While the social and community implications are emergent, there are key directions and concerns that can be identified. With some of these concerns (e.g. data, privacy, inclusive and participatory design), the IoT specific/distinctive aspect needs to further unfold (e.g. with diffusion and take-up). However, there are issues in common with other emergent technologies highlighted in ACOLA Horizon Scanning papers (e.g. Walsh et al., 2019) or in current government inquiries or moves (e.g. ACCC's Digital Platforms Inquiry, the Australian Human Rights Commission's work on Human Rights and Technology). Putting these protections in place is a way to advance issues of trust and consumer acceptance in relation to the IoT. Three key areas which need more attention are smart city developments, RRR locations and engaging Indigenous populations.

5.9.1 Smart city developments in Australia

Cities provide a strategic and convenient context for incubation of the IoT and for identification and public discussion of social implications. The concept of smart cities engages people as householders, citizens, residents, consumers and customers. While there a growing body of literature on how the 'actually existing smart city' is experienced by citizens, very little research has been conducted on this topic in the Australian context. Further research about the ongoing social implications of IoT deployments will be important.

5.9.2 Rural, regional and remote locations in Australia

A broader understanding is needed about the IoT in RRR settings. It is evident from the technology, science, business and other literature that there are important developments occurring across rurally based industries (e.g. precision agriculture, mining, satellite communications). Here again, social research is developing internationally – particularly in relation to farmers' experiences of smart farming technologies – but there is little understanding of how Australian communities have engaged with these developments and what their future impact will be.

5.9.3 Considering viewpoints of Indigenous populations

Engaging and including Indigenous populations in the development of the IoT will require listening to the needs, wants and concerns of community members. Australia has the opportunity to learn from how remote Indigenous communities engage with IoT technologies. In addition to social inequality risks arising from socioeconomic disadvantage and geographic remoteness, Indigenous communities may view some IoT systems as presuming to override their own understandings of the environment and existing data sovereignty. Some data collection (such as visual footage) may conflict with cultural beliefs.

CHAPTER 6
JOBS, SKILLS, EDUCATION AND RESEARCH

Chapter overview

Short-term

- To support training and research, educational institutions will need to develop and maintain an IoT server with the capability to connect to diverse data sources and sensors while providing easy access to students. A supporting cloud and network infrastructure will also need to be enhanced in order to protect data, manage devices and perform data analytics.
- Industry, education providers and governments could consider incentives or measures to attract and retain qualified trainers with the requisite experience in IoT.
- There are specific regional and rural considerations, including connectivity, attracting qualified trainers and supporting Indigenous Australians. However, the location of remote data centres could create new opportunities for investment and employment in regional areas.
- Government could consider supporting SMEs for resourcing and collaboration with industry and education providers, so that employees are well equipped to adapt to and adopt IoT technologies.

Medium-term

- The IoT is likely to create jobs in network design, planning and implementation, cybersecurity, energy management, and data monitoring, management and analytics. Other opportunities include Industry 4.0 and sensor/device design and manufacture.
- Targeted upskilling programs and innovative learning methods can help support employees to bridge skill shortages. Learning methods might include micro-credentials, AR-based training and game-based learning.
- 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 at partner universities.

Long-term

- There is a role for government and the education sector to continually assess the curriculum to ensure that it is future-proof and that the workforce is appropriately skilled for emerging technologies such as the IoT.
- Indirect jobs in cloud services and hosted services are also expected to arise over the next decade.

6.1 Introduction

This chapter considers some of the skill, education and infrastructure requirements to build a workforce and talent pipeline to support a future IoT-permeated economy. This will require innovation and collaboration by government, education providers and industry, as well as ongoing evaluation of existing education infrastructure. RRR communities may face particular challenges such as distance and retention of qualified trainers. Finally, future research considerations to enable a more considered deployment of IoT in Australia are outlined.

6.2 The IoT and the future workforce: potential implications

There is considerable overlap between the IoT and related technologies that have been investigated in recent ACOLA research (e.g. Walsh et al., 2019). It is increasingly recognised that the disruptive impacts of technology are amplified by their interconnectedness in Industry 4.0. The IoT has been described as one of the top five 'disruptive technologies' (including mobile and cloud technology, advances in computing and big data), associated with Industry 4.0 (World Economic Forum, 2016), and has been referred to as its 'heart' (Internet of Things Alliance Australia, 2019). This has important implications for employment, education and training.

The complex and interwoven nature of these issues, and the pace at which the technologies are developing, means that there will also be the need for increased collaboration between industry, educators and governments to improve the responsiveness and flexibility in delivering skills – from formal qualifications to micro-credentials or non-formal education (Evensen et al., 2019; Seet and Jones, 2019b).

6.2.1 Job evolution

There is a lack of agreement about the exact nature of the impact of the IoT and related technologies on the job market. While some see these technologies as offering limitless new opportunities, others argue that they will lead to significant losses of jobs or tasks within jobs (AlphaBeta, 2017; Chartered Accountants Australia and New Zealand and Deloitte Access Economics, 2016; Frey and Osborne, 2013; Institute for Public Policy Research, 2015). The inter-connected nature of these Industry 4.0 technologies (e.g. automated systems working with each other using IoT networks) can lead to multiplier effects, thereby impacting jobs more significantly than just independent uses of these technologies.

6.2.2 Hard versus soft skills

Much of the recent debate related to digital disruption has focused on the dichotomy between the importance of hard or technical skills (such as IoT engineering, cybersecurity, data science and data knowledge) and soft or non-technical skills (design, critical analysis of social issues, problem solving and ethics). This divide is driven by modelling based on a technology-centred (automation) scenario. However, it ignores two other important scenarios, as reported by German researchers: the specialisation and hybrid scenarios (Buhr, 2015; Hirsch-Kreinsen, 2016).

Under the specialisation scenario, people use cyber-physical systems to aid decision making, and the dominant role of qualified workers is maintained. While there will be less need for employees with administrative, production and monitoring competencies, highly qualified and ultra-specialised employees with IT competencies will be required. Given the complexity of IoT technology, future teams will consist of people with deeply specialised skills; very few individuals will have expertise across skill boundaries (GSMA, 2018; Heuss, 2014). To manage these teams, new boundary-spanning skills will be required. Some examples include 'distributed architecture', 'operating systems and embedded systems', 'communications, networks and protocols' and 'mobile computing' (Assante et al., 2018).

Under the hybrid scenario, monitoring and control tasks are performed jointly via cooperative and interactive technologies, networked objects and people. In this scenario, employees will face an increased demand to be highly flexible. Employees with technical skills will need to broaden their outlook to consider the implications of what they design, on the basis that they will be likely to oversee the implementation of the IoT project that they build (Griffith, 2018). In this scenario, the ability to lead, manage and communicate will be critical. The implementation of IoT solutions typically involves significant modification in terms of work content, processes and environment (Assante et al., 2018). This underscores the importance of soft skills, in particular, problem solving, critical thinking, team working, creative thinking and emotional intelligence. Equipping students and workers with these capabilities is paramount to their ability to manage in an environment that is constantly evolving (Turcu and Elena, 2018).

6.2.3 Future IoT workforce

Current research envisages four major areas of future jobs in an IoT-permeated economy (Korom, 2019; van Eck and Waltman, 2010, 2014). These are described in the following sections, with Figure 16 showing an overview of these roles and their requirements.

Network design, planning and implementation

Overview

New roles are likely to be created in the design planning and implementation of IoT across different business sectors.

Job description

Involves the development of systems and frameworks to enable the integration of devices, middleware and platforms into business.

Skill requirements

Will require understanding of network and telecommunications, collaborative problem-solving, and communication skills.

Current role examples

KPMG's IoT consultancy practice offering advice on implementation in smart cities, precincts and campuses, food and fire and energy and natural resources.

Niche opportunities

Opportunities exist for start-ups to develop solutions to challenges of the Australian context such us connectivity solutions for Australia's remote and rural communities.

Security

Overview

New roles in cybersecurity are likely to be created to support the integration of IoT into niche areas, such as the integration of safety monitoring platforms in smart cities and regions.

Job description

Involves the reinforcement of security and safety management of the whole system.

Skill requirements

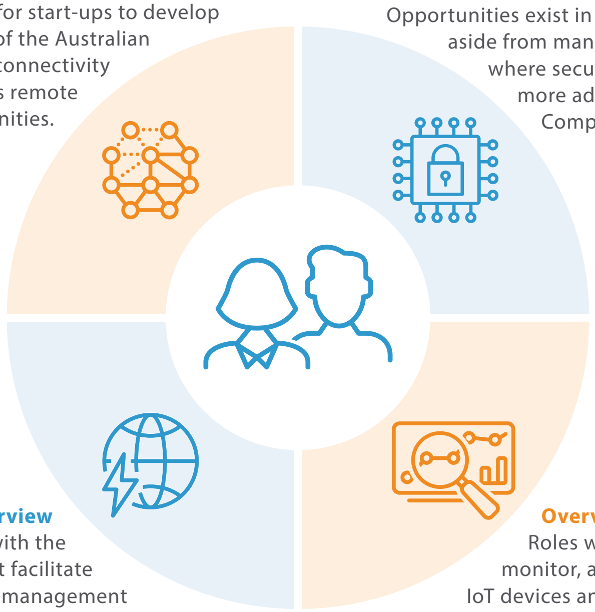
Will require understanding of data analytics, machine learning, IoT hard and software architecture, global security standards, problem solving and risk management.

Current role examples

Vi Dimensions (Singapore) which is developing machine-learning based platforms that use data collected from IoT devices to provide more reliable security for cities enterprises.

Niche opportunities

Opportunities exist in sectors aside from manufacturing and industry where security solutions are more advanced (PwC and the Computer Society, 2018).



Smart energy

Overview

Roles associated with the products and services that facilitate the deployment and management of smart grids, including remote monitoring and management of substations.

Job description

Involves utilising digital grid labs and power distribution software to monitor and manage systems.

Skill requirements

Will require understanding power system engineering, data analytics, advanced infrastructure knowledge, risk management, cyber security standards.

Current role examples

The US Energy Department has invested in a Smart Grid workforce development program to train the future workforce for smart grid management (US Energy Department).

Niche opportunities

Opportunities exist for innovative service models such as Pooled Energy which integrate pool maintenance services with smart energy data analytics for customers (Pooled Energy, 2020).

Data monitoring, analysis and management

Overview

Roles will be created to monitor, analyse and manage IoT devices and ecosystems.

Job description

Involves monitoring and manipulating assets, conditions, and performance management, with sector-specific applications.

Skill requirements

Will require strong understanding of big data, machine learning and predictive analytics, creative problem-solving and communication skills, specific sector knowledge.

Current role examples

Analysis by PwC indicates that monitoring and tracking will form at least half of the major generic IoT use cases, as a consequence of sensor systems integration (PwC, 2018).

Niche opportunities

Opportunities exist to develop niche capabilities in data monitoring and management where Australia has expertise such as healthcare, mining and smart urban/region applications.

Figure 16: IoT jobs of the future

6.2.3.1 Network design, planning and implementation for the IoT

A holistic, emergent and open systems view of networks is required in the planning and implementation of the IoT, to enhance innovation ecosystems (Suseno and Standing, 2018). It is anticipated that jobs will be created to help ensure that network infrastructures are robust, reliable and scalable. First movers in Australia in this area include the 'Big 4' professional services firms, which have re-skilled and transformed many of their digital strategy consultants to take on IoT consultancy roles.

Case study 26: Rethinking core industry capabilities

KPMG Australia started an IoT practice in 2016, covering three core sectors: smart cities, precincts and campuses; smart food and fibre; and smart energy and natural resources. In the absence of sufficient internal experience in this emerging technology, KPMG focused on external hiring of individuals with relevant IoT industry knowledge, expecting to grow its IoT consulting headcount by 50 percent within a year (KPMG, 2018).

A large part of this planning involves jobs within network communications or telecommunications. Most of the underlying IoT connection technology, both in Australia and globally, is developed by large multinationals (e.g. Cisco, GE, Intel, Ericsson, Siemens). As all major mobile operators in Australia have deployed NB-IoT technology and are also rolling out 5G, there will be opportunities for local jobs in the integration and delivery of these new technologies in Australia (PwC and Australian Computer Society, 2018), as discussed in Chapter 6. With the finalisation of the NBN expected in 2020, NBN Co is seeking to build a user-facing technical field force to shift the company's role from network builder to network operator (Crozier, 2019). There may be opportunities to leverage the skills of this existing workforce in the implementation and planning of IoT telecommunications infrastructure.

In addition, given the challenges of the Australian context – long distances and challenges to fibre and mobile coverage across many parts of RRR Australia – opportunities exist for innovators and entrepreneurs to develop creative solutions to improve connectivity. This includes developments in the emerging satellite communications industry, led by companies such as Fleet Space Technologies and Myriota. In 2019, the Australian Government also invested in space and satellite technology through the Space Infrastructure Fund, which is likely to focus industry efforts. Satellite technologies are discussed in more detail in Appendix B.10.

Case study 27: WiFi chip design

Morse Micro, an Australian start-up based at Cisco's Sydney Innovation Centre, has developed a WiFi chip that is cheaper, more powerful and five times smaller than conventional IoT WiFi chips. This may provide better high-speed internet coverage in RRR areas.

6.2.3.2 Security skills for the IoT

The need for skills in cybersecurity is likely to increase as IoT capabilities grow, to provide more reliable security for cities and enterprises. In addition to general IT jobs, specialised jobs in computer vision, object recognition, facial recognition, target tracking, sensor fusion, localisation and mapping, machine translation and deep learning will also be required (Vi Dimensions, 2019).

6.2.3.3 Energy and the IoT

In the energy sector, the IoT's interconnected features will require products and services that facilitate the deployment and management of 'smart grids.' The smart grid will support the employment of smart field workers (Intel, 2019). Instead of working through layers of bureaucracy, operations and maintenance, these personnel will be able to use devices enhanced by AR to gain real-time access to central systems, technical manuals, and even instruction videos, to solve technical field problems without having to wait for appropriately trained personnel. For example, the US Department of Energy has developed a smart grid workforce development program in collaboration with educational institutions and industry (US Department of Energy, 2019). As part of this, the National Electrical Manufacturer's Association, together with George Mason University and Northern Virginia Community College, jointly developed a series of videos dubbed 'Vids4Grids' that provide an overview of the range of new technologies in the energy industry and present insights into smart grid careers at all levels of the energy industry (US Department of Energy, 2019).

6.2.3.4 Data monitoring, analysis and management of the IoT

Given the number of devices and systems connecting to each other and the significant amount of data generated, jobs requiring data analytics skills to monitor, analyse and manage the IoT are growing in number. Analysis by PwC indicates that monitoring and tracking will form at least half of the major generic IoT use cases, as a consequence of sensor systems integration (US Department of Energy, 2019). In a McKinsey job advertisement for IoT Engineers (Operations), the main task of the IoT Engineer was to 'work with teams to develop industry 4.0 solutions for smart manufacturing in cross-sector industrial applications deploying applications such as Digital Performance Management systems, asset tracking and condition monitoring' (McKinsey & Company, 2019b).

6.2.3.5 Other potential role opportunities in IoT

Aside from the key areas above, the IoT will also likely create new employment opportunities in other areas including Industry 4.0 (World Manufacturing Foundation, 2019) and IoT sensor/device design and manufacture (Dettmer and Wieladek, 2019).

6.2.4 Skills training and development

International and Australian evidence highlights challenges in terms of finding workers, particularly graduates, who are trained – or even familiar with – IoT technologies in the industrial usage context (Turcu and Elena, 2018). This is largely a consequence of the complexity and newness of these dynamic technologies, which are constantly evolving (Probst et al., 2018). A Microsoft survey of 3,000 decision-makers across six countries indicated that 47 percent of companies that have adopted IoT solutions feel that they don't have enough skilled workers to support these operations (Microsoft, 2019).

6.2.4.1 University initiatives

The higher education sector has recently begun to recognise this skills gap, creating partnerships with industry to deliver skills and training required for an IoT and Industry 4.0 workforce. Recent developments include:

- NBN Co has partnered with University of Melbourne and University of Technology Sydney to fund R&D in a number of areas including the IoT, smart cities and connectivity and future workforce capabilities.

- James Cook University (JCU) offers an Electronic Systems and Internet of Things engineering degree at the undergraduate level, which combines information technology, electronic engineering and data analytics. Students also benefit from being able to access the NB-IoT research facility, a partnership between JCU and telecommunications giant, Huawei. Consisting of research labs and workshops, the NB-IoT research facility enables students to develop solutions to real-world problems using the NB-IoT standard.
- JCU is also establishing the Cairns Tropical Enterprise Centre, a new multidisciplinary building focused on the application of IoT in areas such as health, agriculture, tourism, environment and the arts.
- The University of Sydney offers an IoT major for their Bachelor of Engineering degrees.
- From 2020, La Trobe University will also offer a two-year Masters level program that integrates technical knowledge with practical learning opportunities. While based in a new IoT teaching lab in Bendigo, students will use Bendigo city as a living lab, working with industry partners to produce and implement IoT solutions and systems.
- In a joint appointment with Cisco, La Trobe University has also appointed a Cisco Chair in Artificial Intelligence and Internet of Things to consolidate research strengths in these areas across a range of disciplines, including IT, Engineering and Mathematical Sciences.
- Swinburne University of Technology is responding to IoT/Industry 4.0 training requirements across the continuum of its VET and higher education offerings. In partnership with the Ai Group, Swinburne has developed the Associate Degree in Applied Technologies to deliver vocational education across the IoT/Industry 4.0 technology stack. Designed as an engineering 'higher apprenticeship' course, topics include M2M communication, IoT, advanced manufacturing processes, automation and robotics, cloud computing, advanced algorithms, smart sensors and cyber-physical systems.
- RMIT University has also partnered with IBM to deliver two online courses in IoT Strategy and 5G for Business to equip IT and business professionals with the skills needed to adopt and capitalise on these technologies.

Internationally, universities in the US, UK and in Europe are beginning to offer IoT and related certificates and Masters programs (FindAMasters, 2019; Stanford, 2019). Universities are also partnering with technology companies that develop IoT solutions (Probst et al., 2018). By integrating online courses from technology companies into the curriculum of a university course, students are able to access the latest in technology, while universities are able to keep abreast of rapidly changing technologies. An example is NASDAQ-listed Parametric Technology Corporation's IOTU.com platform, which offers courses on becoming an IoT developer. Students can learn about IoT and then build apps using Parametric Technology Corporation's IoT solution, ThingWorx (PTC, 2019). In this case, university students are able to access the latest technology and learn alongside industry professionals and developers, gaining hands-on experience in a highly scaffolded environment.

6.2.4.2 Up-skilling the workforce

In order to keep pace with changing technology and reduce the skills gap, education and training – and moreover, continuous learning – are needed to skill, re-skill and up-skill individual workers. Workers will also need to be trained to handle the transition of systems and data from legacy systems to IoT-based systems. Workplaces will need to train and retrain existing workforces; this will be made more complex by the different training preferences of multigenerational forces (Griffith, 2018). Targeted up-skilling programs and innovative learning methods, including AR-based training, game-based learning and micro-credentials, can help employees to bridge skill shortages (Kovács-Ondrejkovic et al., 2019).

With micro-credential courses, individuals learn specific skills and competencies to meet industry-specific needs, without having to invest the usual time and funds required for higher education qualifications. Internationally, a number of short courses and certifications are available from international companies, including IBM, Cisco, Hewlett Packard and Coursera, and some universities.

Australian universities have also begun to explore micro-credentials. Curtin University's micro-credential course, the MicroMasters Program in IoT, comprises six graduate level courses that aim to equip professionals from any field to design IoT solutions relevant to their area of expertise (CurtinX, 2019). Students participate in live discussions with instructors, with remote access to real laboratory equipment for practical sessions. Students who successfully complete all six courses can use the credits towards Curtin's two Electrical Engineering major programs for the Master of Professional Engineering. The University of Technology Sydney also runs short 'Prepare your IoT future' courses as part of its masterclasses (University of Technology Sydney, 2019).

Evidence has demonstrated that those with high proficiency in numeracy and literacy are more likely to get trained compared to workers performing routine-type jobs. It will be important to ensure that current training programs are appropriate and targeted to provide the most vulnerable with opportunities to adapt and develop skills in a changing employment environment (Organisation for Economic Co-operation and Development, 2018b).

6.2.5 Infrastructure considerations

6.2.5.1 Education–industry infrastructure partnerships

For VET providers and universities to support the development of skills needed in the Industry 4.0 context, educational institutions need to develop the requisite curriculum and courses, underpinned by faculty (e.g. instructors and support technicians) with IoT skillsets and knowledge (University of Technology Sydney, 2019). It is likely that educational institutions will need to develop and maintain an IoT server with the capability to connect to diverse data sources and sensors, to provide a learning environment for students (Probst et al., 2018). Supporting cloud and network infrastructure will also need to be enhanced in order to protect data, manage devices and perform data analytics. Educational institutions should seek to collaborate with industry to provide these resources to students.

6.2.5.2 Education–industry–employer collaborations

In the area of skills and training, several initiatives have started that are related to, but not necessarily specifically focused on, IoT. An example of this is the partnership between Swinburne University of Technology's Advanced Manufacturing and Design Centre and Siemens, which provides students with access to leading-edge technology using Swinburne's Factory of the Future. This acts as a key platform for developing and teaching about Industry 4.0 technologies (Seet et al., 2018). This Swinburne–Siemens collaboration has extended to include employer organisation Ai Group, to develop the Industry 4.0 Higher Apprenticeship Program (AiGroup, 2018). In 2019, the Australian Government also allocated $3.6 million to trial a national one-year Diploma in Applied Technologies, developed by Swinburne and Siemens, to boost the skills of 120 workers in small to medium manufacturing enterprises (Minister for Education, 2019).

In consultation with an industry expert, it was noted that the impact of such collaborations on the job market and other flow-on effects will need to be considered, for example, where a particular company may get first choice of graduates if they have a partnership in place with an education provider.

6.2.5.3 Future-proofing the education sector

It will be important for the Australian Government and the education sector to continually assess the curriculum to ensure that it is future-proof and that the workforce is appropriately skilled for emerging technologies such as the IoT (Kovács-Ondrejkovic et al., 2019). Research indicates that current VET and university graduates lack the technical and non-technical skills required for continuous learning, such as sufficient literacy, numeracy and science, technology, engineering and mathematics skills, which adversely impacts their ability to deal with disruptive technologies (Seet et al., 2018).

Educators should also consider how to cater for the different learning preferences of students, as methods for teaching become more diverse with the use of offline and online tools (Kovács-Ondrejkovic et al., 2019). The personalisation of learning is likely to assist in developing approaches to encourage lifelong learning and continuous up-skilling.

6.2.5.4 Shortage of qualified training providers in Australia

Providing the required education and training for IoT is not straightforward, as a consequence of challenges in sourcing qualified trainers with the requisite experience (Seet et al., 2018). Research on Industry 4.0 has indicated the need for trainers and teachers at all levels 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 (Seet et al., 2018).

Case study 28: International collaboration for Industry 4.0 capability-building

As a result of the shortage of training providers in Australia, REDARC Electronics, a South Australian company specialising in R&D and manufacture of electronic projects, has partnered with offshore institutions, such as the German-based Fraunhofer Institute for Industrial Engineering IAO (one of the German-based Fraunhofer Institutes focused on disruptive technologies), to run dedicated sessions on Industry 4.0 capability building. They have also sent staff to conferences and engineers to Japan to study lean manufacturing and Industry 4.0 compatible machine lines.

6.2.5.5 Challenges for small to medium enterprises

Partnering with international education and training institutions is not always feasible, especially for smaller firms, as they may not have sufficient resources, particularly in traditional 'trade' sectors. Thus, disruptive technologies like the IoT may have a more significant impact on skills development for staff of SMEs than on larger organisations (Seet et al., 2018). While larger firms can implement in-house training or even partner with other organisations to help fill skill gaps, smaller firms prefer to hire workers with the requisite skillset, rather than develop them internally. To address this issue in the European context, the European Commission initiated the IoT4SMEs project to facilitate the development of VET-based qualifications that will underpin the digital transformation of European SMEs seeking to adopt the IoT technology (IoT4SMEs, 2019). Thus, there is an ongoing role for government and leading businesses to support SMEs to adapt to the IoT (noting that the CSIRO and government departments are beginning to assist).

6.2.6 Broader impacts of the IoT on the employment sector

6.2.6.1 Supporting meaningful work and improving customer satisfaction

The IoT has the potential to support more engaging and highly skilled work at the firm level, as well as increase customer satisfaction. For example, IoT systems have allowed REDARC Electronics to achieve maximum transparency and seamless contact with customers 'right throughout the business so they can actually see into the business, see their stock, their product going through the process, understand their lead-times, be able to put their schedules into our systems' (Seet et al., 2018). Customers are provided with maintenance and fault analysis service data in near real-time and understand when and where problems are occurring and how to get these fixed. This has led to improved productivity and reduced labour content as a function of:

- machines talking to operators and vice versa, providing real-time information about the process, quality, performance ratings etc.
- software design capabilities that enable the manufacture of products instantly
- configuration and self-analysis of products in real-time
- rapid prototype tooling using 3D printing, which has reduced the process from three weeks to 24 hours.

In non-manufacturing organisations like professional services firms, IoT technologies will enable:

- knowledge sharing within and across teams
- social collaboration and breaking down barriers between different departments
- sustained engagement post-release of products
- continuous improvement and improved customer relationships over the life of the product.

6.2.7 Considerations for rural and regional areas

6.2.7.1 Locating data centres in regional areas

As IoT systems and applications become more common, the storage, hosting and security of data become important considerations. An increasing number of data centres are being established in RRR areas as government organisations and businesses become more cognisant about where data are hosted and by whom (Niesche, 2019). The establishment of regional data centres offers opportunities for government to collaborate with industry for effective data management. Although data centres have previously been concentrated in urban centres of Sydney, Melbourne and Brisbane, there are a number of benefits of locating data centres in RRR areas. Aside from being physically closer to organisations located in RRR areas, regional data centres may be able to increase the resilience of data by 'boosting the geographic area over which it is spread' (Niesche, 2019). Regional data centres may play a significant role in supporting job creation, while ensuring that IT skills remain in these areas. Jobs in cloud services and hosted services are also expected to rise over the next decade (Niesche, 2019).

Case study 29: Regional data centres

A number of data centres have been established across RRR areas. In 2018, the $40 million Pulse Data Centre was opened in Toowoomba, supported by Schneider Electric, Telstra and the Queensland Government. The Australian-owned cloud, data centre and connectivity provider, iseek, recently established the North Queensland Regional Data Centre, supported jointly by industry, local, state and national funding. The NT Government has commissioned a new government data centre in Millner as the NT Government's primary data centre, with a second backup centre established in partnership with Area, a local IT services provider.

6.2.7.2 Lack of qualified trainers

Many VET providers in RRR areas reported that they found it difficult to recruit experienced trainers with relevant industry experience (Australian Government, 2019c). Even universities that have experience in delivering courses in RRR areas may find it difficult to recruit the qualified and trained staff necessary to teach specialised IoT qualifications. It will be important to consider how to address these deficiencies to allow for the expansion of RRR-focused IoT technologies that are currently being trialled (e.g. smart off-grid power solutions in remote WA; Western Power, 2019) and the deployment of the IoT in regions.

6.2.7.3 Challenges for Indigenous Australians

In various reviews, there is recognition that Indigenous Australians, especially those who live in RRR areas, generally enrol in lower level qualifications due to lower language, literacy, numeracy and digital skills (Seet and Jones, 2019a). As the Joyce Review observed, these lower-level qualifications are often a necessary passport to more employment-enhancing qualifications but do not provide a strong pathway into jobs on their own.

To address some of these issues, the Joyce Review noted that flexible and innovative delivery models need to be considered for these areas (Seet and Jones, 2019b). It recommended that consideration be given to expanding or adopting the regional study hub model, which provides infrastructure and academic support to students studying via distance at partner universities. The Australian Government has provided $16.7 million to establish eight study centres, with an additional funding available for five centres in 2019 to support participation in and completion of courses by regional and remote students (Department of Education, Skills and Employment, 2020). Ongoing institution-wide commitment and collaboration between VET providers, universities, external agencies and community networks will be needed in order to achieve high levels of participation and completion for RRR students (Australian Government, 2019c).

6.3 Opportunities and challenges

Given the inter-connected nature of IoT products and services and the disruptive nature of the technology across sectors, closer industry–government–education collaborations are needed to deliver education, skills and training, to support the transition to an IoT-permeated economy. Some collaborative experiments have begun and these point to a willingness in stakeholders to take the initiative to meet future needs (Seet et al., 2019).

It is important for the Australian Government and the education sector to consider future-proofing the national curriculum to ensure students are sufficiently equipped with both hard and soft skillsets. Education providers should consider collaboration with industry and government to:

- attract trainers and teachers with the appropriate skills and knowledge
- access or maintain an IoT server or systems with diverse data and sensors that can be easily accessed for student learning; supporting cloud and network infrastructure will also need to be enhanced in order to protect data, manage devices and perform data analytics.

As it is predicted that IoT applications and systems will be ubiquitous across society, there are likely to be new opportunities for education and jobs 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 at partner universities.

Governments could consider supporting SMEs for resourcing and collaboration with industry and education providers so that employees are well-equipped to adapt to and adopt IoT technologies.

Regional data centres may be able to play a significant role in supporting job creation, while ensuring that IT skills remain in these areas. Jobs in cloud services and hosted services are also expected to increase over the next decade.

International collaboration and opportunities for investment should also be considered in the development of a domestic IoT industry.

6.4 Future research considerations

Investment in research will encourage innovation and enhance our understanding of the social impacts of the IoT. Alongside government investment, private sector investment will facilitate greater opportunities commercialise research outcomes for the benefit of society. Research organisations should therefore deepen their engagement with industry to encourage collaboration. Understanding the benefits and limitations of IoT applications, and ways to mitigate the potential harms, will ensure that products and services are deployed responsibly and effectively over the next decade. Areas of research to enhance positive outcomes from the IoT for Australia from this report have been consolidated below.

6.4.1 Novel applications of the IoT

Research into novel applications of the IoT will help Australia to grow a domestic IoT industry and encourage innovation, enabling Australia to participate in global IoT markets.

6.4.2 National estimates of IoT devices in Australia

Research on the number and nature of IoT devices in Australia is an area for further research recommended by this report as current figures are still mainly based on industry estimates.

6.4.3 Economic research into the IoT

Further economic analysis of IoT adoption and innovation should focus on the microeconomic aspects of information economics, transaction cost economics and industrial organisation, as opposed to using macroeconomic models that focus on expenditure.

Further analysis on the value of data produced under different property rights regimes and under different regulatory environments would be useful, including considering the distributional consequences of the growth of data assets.

6.4.4 Multi-modal communications solutions for robust connectivity

It is important for governments to consider further research into multi-modal communications options including robust redundancies. Reliable connectivity is critical for essential services and emergency management. This is a particularly significant issue for RRR areas, where telecommunications infrastructure may be at greater risk of damage during environmental disasters such as bushfires. Options to explore include ensuring that legacy connectivity options are maintained, such as the use of copper-wire networks, or exploring new solutions to create aerial wireless networks such as high-altitude balloons (e.g. Project Loon, see Appendix B.10.2.2) or other satellite technologies.

6.4.5 Social research on the impacts of IoT

At present, the evidence on how the IoT interacts with social change factors in the Australian context is still unclear. More research needs to be conducted on the social, cultural and geographical dimensions of IoT use across the broad range of potential domains of use in Australia, including farming, education, transport and industry, as well as smart homes. This is required to fill current gaps in knowledge about how Australian consumers across these domains understand what is meant by the IoT, what benefits they are gaining from these technologies, what risks and harms might be affecting their use or avoidance of IoT technologies, and what developments and improvements they would like to see in the IoT to better suit their needs. Three key areas which need more attention are smart city developments, RRR locations and engaging Indigenous populations.

6.4.6 Smart city developments in Australia

Cities provide a strategic and convenient context for incubation of the IoT and for identification and public discussion of social implications. The concept of smart cities engages people as householders, citizens, residents, consumers and customers. While there a growing body of literature on how the ‘actually existing smart city’ is experienced by citizens, very little research has been conducted on this topic in the Australian context. Further research about the ongoing social implications of IoT deployments will be important.

6.4.7 Rural, regional and remote locations in Australia

A broader understanding is needed about the IoT in RRR settings. It is evident from the technology, science, business and other literature that there are important developments occurring across rurally based industries (e.g. precision agriculture, mining, satellite communications). Here again, social research is developing internationally –

particularly in relation to farmers' experiences of smart farming technologies – but there is little understanding of how Australian communities have engaged with these developments and what their future impact will be.

Further research and ongoing evaluation of current Australian Government initiatives, including the Universal Service Guarantee, Mobile Black Spot Program and the Regional Connectivity Program, is recommended to ensure efficacy in RRR areas. The assessment of emerging technologies such as LEO satellites is also suggested.

6.4.8 Considering viewpoints of Indigenous populations

Engaging and including Indigenous populations in the development of the IoT will require listening to the needs, wants and concerns of community members. Australia has the opportunity to learn from how remote Indigenous communities engage with IoT technologies. In addition to social inequality risks arising from socioeconomic disadvantage and geographic remoteness, Indigenous communities may view some IoT systems as presuming to override their own understandings of the environment and existing data sovereignty. Some data collection (such as visual footage) may conflict with cultural beliefs.

6.4.9 Environmental impacts

The environmental impact of IoT devices should be further explored, given the projected exponential growth of devices over the next decade. This could increase the volume of e-waste exponentially. Sustainable design approaches or mitigation strategies should be explored to ensure that issues such as vendor lock-in, virtual wear out and planned obsolescence are addressed.

6.4.10 Connected and automated vehicles

The deployment of CAVs over the next 10 years will require ongoing assessment of issues such as backward compatibility with existing infrastructure and vehicles. Further research into consumer acceptability and barriers to the uptake of CAVs in the Australian context, as well as related considerations into changes in employment and community conditions would also be beneficial. Potential opportunities to deploy CAVs to improve existing road safety and emergency management systems in Australia, particularly to improve road safety in RRR areas, should also be considered.

6.4.11 Ongoing research on radiofrequency electromagnetic energy related to 5G

No health effects are expected from exposure to RF EME related to 5G. It is, however, important to continue the research in order to reassure the Australian population. The Australian Radiation Protection and Nuclear Safety Agency (ARPANSA) has provided recommendations for areas of research to expand existing knowledge, including the ongoing assessment of personal and environmental exposure to radio waves from new and emerging technologies such as the use of millimetre wave spectrum (Australian Radiation Protection and Nuclear Safety Agency, 2017).

CHAPTER 7
CONCLUSION

Australia is well positioned to derive significant benefits from the deployment of the IoT, including increased productivity, optimised processes and improved liveability of our cities and regions. The volume and veracity of data collected from IoT devices and systems will enable greater understanding and insight across a range of systems and processes. The benefits of the IoT are already occurring – in the improvement, management and monitoring of our utility systems, roadside infrastructure, agricultural products and homes. As this technology matures and data analytics become increasingly sophisticated, governments, industry and consumers will be able to further enhance their decision making, and drive innovation and research. Developments over the next decade include increasingly advanced management of our energy and utility systems, optimised and cost-effective service delivery in our cities and regions, the deployment of CAVs and a new advanced manufacturing sector featuring the use of digital twins.

The use of IoT-enabled service delivery in cities and regions has the potential to improve service delivery, from optimising waste management to improving our prevention of and response to extreme weather events. However, it will be important for governments to take into account emerging issues to maintain community trust and acceptance. Understanding and mitigating the risks of smart system failures and security breaches will be important, given the scale of potential harm that could occur. Increasing dependence on major technology companies by governments may merge private and public interests in the provision of service delivery and could lead to the growing politicisation of urban governance and data management. It is important that the Australian Government consider national leadership and coordination across the three levels of government to consider the ongoing provision and impacts of the IoT, building on existing investment. This will also need the support of relevant industry and community stakeholders, and investment and support for trials and demonstration projects.

Broader social considerations for IoT deployment will include data collection, privacy and equality of access, as well as the impacts on vulnerable populations and on those who may choose to opt out. Further research on the social impacts of IoT use across domains will be required as the technology matures. In addition, the deployment of IoT systems in Australia is contingent on sufficient and available connectivity in both our cities and regions and will be an area for ongoing focus and attention. Australian governments and industries must continue to take a measured response to these issues, by looking to international developments and proactively

engaging with communities and specific cohorts to consider user-centric design and accessibility for products and services.

Australia is well-placed to create a successful national IoT industry, building on our culture of innovation and expertise in sectors such as health, agriculture, environmental monitoring and mining. While global leaders are focusing on the provision of hardware and horizontal software solutions, Australian companies should consider developing niche industry-specific applications or complementary products for existing services by major technology providers. There are also opportunities for new roles to occur in network design, planning and implementation, cybersecurity, energy management, and data monitoring, management and analysis. Both 'hard' technical skills and 'soft' non-technical skills will be required to support this transition.

International standards, while currently heterogenous, are continuing to be refined. Collaboration by industry leaders and work by international standards bodies is encouraging. It would be useful for the Australian Government and industry to continue to monitor these developments to ensure ongoing participation in the global market. National standards could be principles-based, flexible and future-proof. However, security and data will be ongoing concerns and new risks will arise, and the Australian Government could consider the establishment of baseline security measures for IoT-applications and the development of national data standards. It would be useful to ensure that these are consistently reviewed to account for emerging IoT-applications.

There are many lessons that can be learnt from countries that have been successful in the implementation of IoT systems and networks, such as the EU, Germany, UK and South Korea. Shared learnings and considering the factors for success in the adoption and acceptance of the IoT will be valuable for Australia, as well as continued collaboration and investment in research and innovation in a national IoT sector.

The development of a national approach would assist Australian governments, industry and communities on areas where prioritised efforts would be beneficial. It would also help to ensure that IoT technologies are deployed safely, ethically and effectively in our cities and regions. This should provide guidance to all stakeholders on the issues outlined in this report to facilitate ongoing innovation, adoption and acceptance over the next decade, enabling Australia to maximise the positive outcomes from this technology.

APPENDIX A
INTERNATIONAL CONTEXT

A.1 Global IoT trends

Due to the emerging nature of the IoT, there are few evidence-based criteria or metrics to assess global IoT adoption, impacts, trends and maturity. However, some information is available (such as consultancy reports) that can provide an indication of emerging opportunities and global trends.

Technology readiness assessment is a systematic, metric-based process that assesses the maturity of, and risks associated with, critical technologies. Originally developed by NASA, the technology readiness assessment is useful for assessing the development of early forms of new technology. However, it does not assess adoption by users, which is a key factor in the sustainability of emerging technologies.

The technological life cycle can provide a good indication about the development of the IoT. The technological life cycle is composed of four phases:

- R&D phase
- the ascent phase
- the maturity phase
- the decline.

The following section looks at some the key developments in the European Union, UK, USA, China, Japan, and South Korea.

A.2 European Union

The EU has been an early advocate for research and innovation, recognising the IoT as the next step of disruptive digital innovation. It has pushed IoT-related initiatives on standards and cybersecurity since 2005 (Tanczer et al., 2019). Key activities include:

- The Alliance for Internet of Things Innovation was established in March 2015 to support the creation of a European IoT ecosystem (European Commission, 2016). The Digital Single Market was also launched and recognised the need to avoid fragmentation and to foster interoperability for IoT (European Commission, 2019).
- There has been significant funding for IoT research, innovation and deployment projects. €500 million from the Horizon 2020 Programme (2014–21) has been dedicated to addressing the technological, regulatory and societal aspects of the IoT. These research 'clusters' include smart cities, smart farming, energy, digital health and care.
- Germany has led the IoT industrial space, with the development of Industry 4.0 since 2013. Other efforts include Smart Industry in the Netherlands and Slovakia, Fabbrica Intelligente in Italy and Nouvelle France Industrielle (Industrie du Future) in France.
- The 5G Action Plan was adopted in 2016 with the objective to launch 5G in all EU member states by the end of 2020, with rapid deployment of coverage in urban areas and transport areas by 2025.
- The European Cybersecurity Act came into force in June 2019, which established the EU Agency for Cybersecurity ENISA, as well as the European cybersecurity framework. This supplements the General

Data Protection Regulation that mandates a 'Privacy by Design' approach for all IoT solution and products.

- The European Commission Expert Working Group on Liability and New Technologies has recently assessed the impacts of the IoT on existing liability regimes and how they can be improved to meet the emerging challenges from digital technologies.

A.3 United Kingdom

The UK's approach to the IoT has been one of minimum intervention, with the goal of a self-regulated market, although industry has not yet agreed on a single set of principles for data protection, security and safety (Tanczer et al., 2019). However, cybersecurity, particularly for consumer IoT devices, has emerged as a key priority for the UK Government. Key activities include:

- In 2015, the UK Government invested £40 million into the IoT, with £32 million of that investment to establish IoTUK, a national program to amplify UK's IoT capability and increase adoption of IoT technologies and service.
- Establishment of the PETRAS IoT Research Hub, a consortium of nine leading UK universities to study IoT security and privacy issues.
- Amendments to data protection laws in the UK including the Data Protection Act 2018 and ongoing cybersecurity policy development that complements EU regulations and such as the General Data Protection Regulation and Digital Single Market Strategy.
- Existing regulation frameworks apply to data protection, security of networks and information systems, product safety and liability laws, radio equipment safety rules, as well as the emergence of domain-specific legislation such as the Vehicle Technology and Aviation Bill.
- In 2018, the UK Government released 'Secure by Design'. This code of practice for consumer IoT security provides guidance for manufacturers and consumers, noting the need for systems to be updatable, communication data to be encrypted, and attach surface to be minimised. In 2019, the UK Government held consultations on these regulatory proposals. Following this consultation and analysis of the responses received, the government will make a decision on which measures to take forward into legislation. A final impact assessment will be published alongside the decision.
- In 2019, Innovate UK held a funding competition (worth £6 million) for UK businesses to develop collaborative R&D projects addressing major IoT cybersecurity challenges.
- An investment of £1.9 billion (2016-21) into the National Cyber Security Programme including the establishment of the National Cyber Security Centre.
- In 2019, the UK Government committed to a £70 million investment to support cybersecurity research into hardware and chip designs at development stage. A further £30 million investment to ensure safety and security of IoT devices with £420 million to be deployed across the UK over the next three years.

A.4 United States of America

Emphasis in industrial IoT has predominantly focused on the IT aspects of the top layer, such as cloud computing, big data and VR (Zhong et al., 2017). Governance and policy has been disparate, with multiple agencies driving cybersecurity and innovation policy (Chatfield and Reddick, 2019). Many experts have urged the US Government to avoid over-regulation that could limit innovation in the

IoT market and prevent economic benefits to US business and consumers (Chatfield and Reddick, 2019). Key activities include:

- The Industrial Internet Consortium was established in 2014 to support industrial IoT by multinationals GE, AT&T, Cisco, Intel and IBM.
- There have been multiple projects to support the development of the IoT through standards, interoperability and cybersecurity since 2013 by federal departments, including the Federal Communications Commission, the Federal Trade Commission and the National Institute of Standards and Technology (Chatfield and Reddick, 2019).
- Cybersecurity remains a key concern, but while several bills have been introduced to Congress, none have made it to a vote. The IoT Cybersecurity Improvement Act of 2017, which aims to set minimum security standards for connected devices purchased by government, was reintroduced to the House of Representatives in 2019 (Robertson, 2018).
- California became the first state to pass a state IoT cybersecurity law in August 2018, mandating that all devices must be equipped with 'reasonable' security features, including having a unique password for each device (SB-327 Information Privacy: Connected Devices, 2018).
- In 2019, the US Congress introduced a number of proposals to study and cultivate the growth of smart cities and how these technologies could improve congestion, utilities and buildings (Discher and Ponder, 2019).
- The world's first commercial 5G service was launched in 2018.
- The Federal Communications Commission is in the process of allocating additional high-band spectrum, mid-band spectrum, low-band spectrum and unlicensed spectrum (Hogan Lovells, 2019).

A.5 China

China is emerging as a global leader in innovation and adoption of the IoT (Kshetri, 2017). The Chinese government views the commercial success of Chinese firms as an indicator of political legitimacy and economic modernisation. This has led to a proactive authorising environment that has supported the development of the IoT industry (Kshetri, 2017). Key activities include:

- In 2014, the Chinese government invested US$1.6 billion in the IoT, with further plans to invest more than US$600 billion by 2020 in M2M solutions and other fields in this sector.
- The 'Made in China 2025' strategy aims to promote domestic integration of digital technologies and industrialisation to develop the Industrial Internet.
- As of 2014, over 90 percent of China's provinces and municipalities have listed the IoT as a pillar industry (Kshetri, 2017). However, successes have been dependent on political and institutional support from the Chinese Communist Party (Yu and Xu, 2018).
- The 13th Five Year National Plan (2016-20) outlined the development of the IoT as part of Internet+ priority (Zhong et al., 2017).
- Public awareness of rights to privacy is less developed than in countries such as the US, which may provide institutional advantage in the Chinese IoT market (Kshetri, 2017). However, there is also a lower degree of trust in the government: households are installing their own air quality and pollution sensors due to mistrust of agencies' reported statistics on environmental pollution (Kshetri, 2017).

A.6 Japan

Japan has focused on how the IoT can better support demographic change, with an ageing population and the associated implications for health and wellbeing and the economy (Forbes, 2018). The lead-up to the 2020 Olympic Games was also been a key driver for ensuring that cyberspace is 'free, fair and secure' for all (The Government of Japan, 2015). Key activities include:

- Japan launched an Industrial Value Chain Initiative, in alignment with Germany's Industry 4.0 initiative in 2015. This brings together 30 Japanese manufacturers to encourage collaboration and discuss how human-centric manufacturing will change with the IoT (Zhong et al., 2017).
- The Japanese Government launched the Society 5.0 Strategy in 2017 to 'create a new social contract and economic model' by incorporating new technologies (Davies, 2018). The interconnectedness and big data derived from the IoT is expected to improve outcomes in health, urban mobility, logistics and management of infrastructure (Davies, 2018).
- In 2019, the Japanese government launched a nationwide experiment to test the security of internet-connected devices owned by citizens and businesses by using default credentials to log into devices, without prior consent. Owners of vulnerable devices are then warned by their internet service providers. This has caused controversy due to the lack of individual consent, but is due to run until 2022 (Boyd, 2019).

A.7 South Korea

South Korea is one of the most networked countries in the world, making it an attractive test-bed for IoT applications for both local and global firms. South Korea released its Master Plan for Building the Internet of Things in 2014, which outlined a national strategy including the development of open platforms, leveraging open innovation and global collaboration. The rollout of IoT-dedicated networks by Telcos has made IoT projects more feasible for government investment. Key activities include:

- The South Korean Government announced that it would create an IoT and smart car industry by 2024 that will be worth ₩100 billion (US$90 million) (Mu-Hyun, 2015).
- Since 2014, an IoT Roadmap to develop cybersecurity standards and best practices, an IoT Security Alliance, and an IoT-Information Sharing and Analysis Centre have all been established.
- In 2016, the Ministry of Trade, Industry and Energy announced that it would invest ₩7 trillion in 12 R&D sectors, including the IoT, as future growth engines in partnership with the private sector (Australian Trade and Investment Commission, 2020).
- Since 2016, telecommunications carriers including Korea Telecom, SK Telecom and LG UPlus have been active in expanding IoT partnerships with local service providers in different sectors by using their networks (Australian Trade and Investment Commission, 2020).
- There has been a broader deregulatory campaign, aimed at boosting economic growth to lower barriers for businesses in the IoT sector and to promote early establishment of nationwide networks dedicated to the IoT(Australian Trade and Investment Commission, 2020).
- The city of Songdo was one world's first 'smart cities', developed in 2016 as a sustainable, low-carbon high-tech city with sensor networks monitoring energy use, traffic flow and healthcare.
- In 2019, it was announced that the Metropolitan Government of Seoul would deploy an enterprise-grade city-wide IoT network using LoRA devices and a LoRaWAN protocol to create a hyper-connected city by 2022 (Ribeiro, 2019).

APPENDIX B
TECHNOLOGY

B.1 Enabling architecture

The IoT is not the result of a single novel technology. Instead it consists of several complementary technical developments to bridge the gap between the virtual and physical worlds. An IoT device commonly consists of a sensor and/or actuator, communication infrastructure and a processing unit. While the IoT device itself is a critical component, it is important to understand that it acts within a system of enabling architecture to perform the wider applications that we ascribe to the IoT. Table 2 expands on the discussion of IoT architecture in the introduction: it notes the components in each layer and their associated tasks, as well as the different services, networks and protocols involved in the different IoT architecture layers (Da Xu et al., 2014).

B.2 Interoperability

In the development of IoT networks, a major problem is the integration of heterogeneous objects (Vega-Barbas et al., 2012). This is known as interoperability. Interoperability is defined by the IEEE as 'the ability of two or more systems or components to exchange information and to use the information that has been exchanged' (Radatz et al., 1990, p. 3). Improving the interoperability of IoT networks is crucial. Big vendors (such as Amazon, Cisco, IBM and Apple) have dominated the IoT market. However, they all use different IoT platforms and each has its own protocols and interfaces, which are not compatible with each other. According to the European project Unify-IoT, there are more than 300 IoT platforms in the IoT market (Unify-IoT, 2016). The lack of interoperability causes multiple problems in IoT networks, including vendor lock-in, difficulty in plugging IoT devices to non-compatible platforms, and the lack of cross-platform and cross-domain IoT applications (Noura et al., 2019).

Table 2: Detailed architecture layers, components, tasks and protocol

Layer	Components	Tasks	Protocol used
Perception/device layer	Sensors (temperature and humidity) and actuators (motor and relays)	Identify, monitor, acquisition and action	LTE-A, EPCGlobal, IEEE 802.15.4, Z-Wave, Bluetooth, 802.11 WiFi
Network layer	Nodes, gateways, firmware	Device management, processing and secure routing	MDNS, DNS-SD, RPL, 6LoWPAN, IPv4/IPv6
Service layer	Vendor specific third party application	Machine learning, processing, pre-processing and real-time action	
Application layer	Third party application, websites, consoles and touch panels	Machine learning, business models, graphs and flow charts	HTTP, CoAP, DDS, AMQP, MQTT, MQTT-SN, XMPP, HTTP REST

B.3 Communications technologies for the IoT

IoT devices are connected to each other by communication networks (the network layer of the enabling architecture, see Table 2), enabling the transfer of the data and action between device and middleware collection, analysis and action on data without human intervention. Communication technologies are therefore often considered the backbone of IoT infrastructure. This section compares different communication technologies and examines potential technology advancements.

These connectivity technologies range from well-established networks such as WiFi and 4G to the latest deployments such as 5G, as well as emerging networks such as Sigfox, LoRa and NB-IoT. Telstra and Thinxtra (the Sigfox licensee in Australia) are currently the leading IoT connectivity providers in the Australian market. Telstra is presently dominating the market given the strong coverage of their 4G cellular footprint. Popular communication technologies for the IoT are outlined in Table 3 (Elkhodr et al., 2016; Ray, 2018; Sinha et al., 2017).

B.3.1 WiFi

WiFi is among the first technology choices for supporting the IoT, with the dominant existing services providing data rates from 1 Mbps to 1 Gbps, with transmission ranges of around 20 m indoors and 100 m outdoor (Ray, 2018). However, in many IoT applications, IoT devices have limited hardware capability, low power consumption and low cost requirements. WiFi is generally a power-intensive method of communication and may not be appropriate for all applications. As such, low-cost and low-power wireless technologies are needed.

B.3.2 Zigbee, Bluetooth and LoRa

Zigbee and Bluetooth (or Bluetooth Low Energy) are suitable for portable devices for a low data rate application (generally less than 1 Mbps) with limited battery power over short ranges (less than 20 m). Bluetooth can provide a slightly higher data rate but a reduced number of nodes (i.e. eight nodes per network/piconet). Zigbee can support more nodes; however, it has limited computing capacity of devices.

Table 3: Comparison of communication technologies for the IoT

	Standard	Channel bandwidth	Data rate	Latency	Transmission range	Energy consumption	Cost
Cellular network	4G: LTE	5–20 MHz	DL: 0.1–1 Gbit/s UL: 50 Mb/s	10–100 ms	Cellular coverage area	High	High
	5G: NR	Up to 800 MHZ	1–20 Gb/s	1–5 ms		High	High
Cellular IoT	LTE-M: 3GPP R12, R13, R14	1.4 MHz	1 Mb/s	10–15 ms	11 km	Low	Low
	NB-IoT: 3GPP R13, R14	180 kHz	250 kb/s	1.6–10 s	35 km	Very low	Low
WiFi	IEEE 802.11a/b/ g/n/ ac	20–40 MHz	1 Mb/s–1 Gb/s	10–100 ms	20–100 m	High	High
	IEEE 802.11ah	1–16 MHz	0.3–347 Mb/s	10–100 ms	1 km	Low	Low
WiMAX	IEEE 802.16	1.25–20 MHz	1 Mb/s–1 Gb/s	50 ms	<50 km	Medium	High
ZigBee	IEEE 802.15.4	2 MHz	40–250 kb/s	60–100 ms	10–20 m	Low	Low
Bluetooth	IEEE 802.15.1	1 MHz	1 Mb/s	60–100 ms	8–10 m	Bluetooth: medium BLE: very low	Low
LoRA	LoRa (PHY) LoRaWAN (Networking layer)	125–500 kHz	0.3–50 kb/s	1–15 s	15 km	Very low	Low

The emerging LoRa technology, developed by the LoRa Alliance, is intended for the LPWAN (Lavric and Popa, 2017). LoRa uses chirp spread spectrum modulation, which can support a large transmission range of up to 15 km with a relatively low data rate of 0.3-50 Kbps, using the unlicensed ISM frequency band. Moreover, LoRa has a very high capacity to receive messages from a large number of end nodes. As of January 2019, more than 100 network operators have deployed and operate public and private LoRaWAN networks (LoRa Alliance, 2019).

B.3.3 Cellular IoT

Aiming at LPWAN, cellular IoT technologies developed by the 3rd Generation Partnership Project include LTE-M and NB-IoT. Among these protocols, NB-IoT is the most recent and was standardised in 2016. The deployment options for NB-IoT are flexible:

- standalone, reusing the 200 kHz bandwidth of Global System for Mobile Communication
- guard-band, using the guard band of two adjacent LTE carriers
- in-band, 200 KHz of the LTE band is reserved for NB-IoT.

While LoRa works in the unlicensed spectrum, NB-IoT operates in licensed bands and can provide better quality of service at the expense of higher cost. NB-IoT is better suited to applications requiring higher quality of service. NB-IoT has a lower latency because of the infrequent but regular synchronisation with the base station but consumes extra energy and therefore has a lower battery life than that of LoRa (which operates in an asynchronous way).

Applications that are sensitive to latency and require higher data rates would benefit more from NB-IoT. As of March 2019, over 100 operators in 53 countries have deployed or launched either NB-IoT or LTE-M networks (Global Mobile Suppliers Association, 2019).

B.3.4 Evolving from 4G to 5G

In comparison to WiFi, 4G can provide better quality of service, support mobility and provides large area coverage. Emerging 5G cellular networks provide connectivity for three scenarios:

- enhanced mobile broadband, which improves data rates and capacity of 4G
- massive machine-type communications, for massive number of IoT devices in dense urban environments with low data rates and limited computing resources
- ultra-reliable low-latency communication (URLLC) which intends to provide extremely high reliability with very low latency.

Using software defined networking, network function virtualisation, and mobile edge computing, 5G will enable network slicing to support multiple communication networks, optimised for different services over the same physical infrastructure. For enhanced mobile broadband, a peak data rate can reach 20 Gbps, which is targeting high speed mobile connections and supporting emerging virtual/augmented reality services. Machine type communication will support smart metering, transport logistics and environment monitoring.

In contrast, 4G generally operates at up 28 Mbps. 5G could even replace many landline connections, and base stations will be able to handle up to a million connections, versus the 4,000 that 4G base stations can cope with. These advances in technology could make communications at live-streaming events much more accessible.

5G will provide URLLC, which can support wireless control IoT technology and enable widespread efficiencies and improvements across many industries. Consequently, 5G is considered one of the key pillars of the fourth industrial revolution or Industry 4.0. URLLC in 5G is poised to provide 1 ms end-to-end delay and reliability of 99.999 percent, compared to more than 50 ms latency in 4G and network reliability of 95 percent.

B.4 Wired technologies for the IoT

There are still some scenarios where wired communications are employed for IoT applications, such as building automation, power utility and industrial automation (Flammini et al., 2009). Various wired 'fieldbus' systems have been developed, most of which are very simple, with a data rate of 1–10 Mbps and a transmission range of less than 100 m. However, these systems are incompatible with Ethernet or IP-based local area networks, which becomes a barrier to integration with external internet. As such, a new wave of Ethernet-based networks has emerged with a larger data rate of 100 Mbps. The wired network is traditionally considered to be more reliable than wireless networks and can be used to supply electric power at the same time. Fixed networks connect gateways to the cloud or data centres, while wireless networks operating in license free bands, such as Zigbee and WiFi, could provide local connectivity, between sensors and gateways.

B.5 Spectrum considerations

Radiofrequency spectrum and allocation of frequency bands is critical for Australian communications and media industries, as increasing numbers of services and activities are relying on wireless connectivity. The emerging and existing wireless technologies are continuously driving demand for spectrum, including 5G cellular networks, IoT applications and smart satellite technologies. To meet this challenge, ACMA endeavours to provide efficient and effective spectrum management to maximise the economic benefits in their five-year spectrum outlook report which is released annually. The most recent publication is their 'Five-year spectrum outlook 2019–23' (Australian Communications and Media Authority, 2019b).

B.5.1 Wireless broadband, including 5G

5G will use spectrum across a wide range of frequency bands, including low-band spectrum below 1 GHz, mid-band spectrum between 1 and 6 GHz, and high-band millimetre wave band (24–86 GHz) (Flore, 2017). Below 1 GHz, ACMA aims to optimise the efficient configuration of the existing 850 and 900 MHz band allocations. The mid-band between 1 and 6 GHz is currently the focus of 5G deployments, particularly around 3.4 to 3.7 GHz. In December 2018, ACMA allocated 125 MHz of spectrum in the 3.6 GHz band (3575–3700 MHz) in metropolitan and regional areas. The 3.4 GHz band, which has already been allocated, will also be used to deliver 5G. In 2019, ACMA sought public consultation on the reallocation of 3700–4200 MHz for wireless broadband services, including 5G, as well as the consolidation of different licence arrangements to facilitate more efficient use of spectrum and a reduction in network deployment costs.

In the millimetre wave band, ACMA is currently focusing on the bands 26 GHz and up. Higher frequency bands have significantly reduced range compared to lower frequency bands. Signals in higher bands will have a range of a few hundred metres and do not penetrate doors or windows, so provide poorer indoor connectivity. Bands from 24 GHz and up will likely be used in short-range indoor applications and dense inner-urban areas only.

B.5.2 Machine-to-machine communications

The IoT can use frequency allocations across the entire spectrum. There are several existing and new radio access technologies for low data rate, long range, power efficient, time non-sensitive massive IoT applications. Devices providing industrial metering, switching and control (including smart infrastructure) feature very low data rates and operate in LPWAN. In the licensed spectrum category, there are three technologies to support massive IoT: extended coverage GSM Internet of Things (EC-GSM-IoT), supported on the existing GSM (2G) equipment and frequency bands; LTE-M, based on 4G technology; and NB-IoT. In the unlicensed spectrum, there are two proprietary wireless technologies for massive IoT: LoRA, mainly deployed in Europe, and Sigfox, with limited applications in the US.

B.5.3 New approaches to spectrum sharing

Across Australia and globally, demand for access to spectrum by new and increasingly sophisticated wireless technologies (such as 5G cellular networks and IoT applications) continues to put pressure on current strategies for spectrum management. Dynamic spectrum access (DSA) based spectrum sharing could be an important component of an effective spectrum management regime and could be used as a tool to maximise the benefits achieved through use of the spectrum resource. However, the technology has not been adopted yet in wireless standards. Some government regulators such as the US Federal Communications Commission and Ofcom (UK) have proposed a specific DSA framework, where secondary users monitor, identify and exploit instantaneous spectrum opportunities with no, or limited, interference to primary users. Industry and standardisation initiatives, under the auspices of major regulatory agencies, have mobilised to bring such management concepts into standardisation, including anearly standard version of IEEE 802.22 and new standards such as IEEE 802.11af and ECMA-392. Notably, these standards have been designed for specific TV white space, where a device can obtain an available channel list from a TV white space database.

Due to technological constraints such as hidden node problems and interference control, the DSA implementations to date are limited. Government regulators will continue to monitor technical developments, and investigate and implement DSA when and where appropriate. ACMA is currently reviewing new approaches to spectrum sharing after public consultation in 2019 (Australian Communications and Media Authority, 2019c).

B.6 Data analytics platforms

IoT big data and analytics requirements have exponentially increased over time and promise improvements in decision-making processes. To facilitate the combination and integration of huge volumes of machine-generated sensor data, one priority will be to provide reliable and seamless connectivity. There must also be efficient storage techniques to handle large amounts of unstructured data in real time and in low-cost hardware. Additionally, due to a variety of system protocols of wired, wireless and hybrid type in a dynamic networking environment, the IoT demands quality of service requirements from conventional homogeneous networks. Integrating quality of service architecture into the IoT is another key requirement for efficient data analytics. Finally, streaming analytics has rapidly emerged as a key IoT initiative for timely decision-making processes. Big data implementations that perform analytics with real-time queries should help organisations interact with people and other devices, quickly obtain insights and speed decision making.

There is a growing array of off-the-shelf big data processing and analytics platforms, ranging from sector-specific applications to bespoke options for businesses. The following are examples of several big data processing and analytics platforms suitable for large amounts of IoT-generated data. Hadoop is an open source data processing platform that stores and processes large amounts of data on a cluster of commodity hardware (Nandimath et al., 2013). The core components, Hadoop Distributed File System and MapReduce are used to store the data and to process the data in a distributed manner, respectively. Another platform is 1010data, which provides advanced analytic services for large-scale infrastructure, including optimisation and statistical analysis (Morabito, 2015). In addition, SAP-Hana (Färber et al., 2012) and HP-HAVEn (Burke, 2013) can also be used as big IoT data platforms.

B.7 Hardware capacities

Advances in the Industrial Internet are accelerating the development of the IoT through an increase in network agility, integrated AI and the capacity to deploy, automate, orchestrate and secure diverse use cases at hyperscale. One of the basic requirements is to have the capacity for millions of devices, machines and computers to communicate in a massive network, sometimes across large distances. Aside from ubiquitous connectivity, the IoT requires cheap, low-powered and secure hardware to flourish (Manyika et al., 2015).

While many applications for IoT are technically achievable, a key barrier has been the cost of components such as sensors nodes. However, with the cost of microelectromechanical systems (a core sensor component) decreasing yearly, the IoT hardware segment is rapidly increasing in sophistication, in terms of sensor capabilities, battery life, security and processing power.

It is anticipated that in the future, a cheap, unified sensor will monitor several variables, rather than multiple sensors each taking a single measurement. While there has been interest in using ambient energy (Briner, 2019) to recharge capacitors or batteries, the lifespan of rechargeable batteries has been a limiting factor; this is expected to be resolved in the future. New state-of-the-art security approaches using encryption keys and secured protocols such as blockchain or quantum cryptography (Mcgrath, 2019; Nelson, 2019) will be integrated in the design of IoT hardware sensors, to further enhance current hardware security. Future intelligent sensors will require a computational processing unit to make decisions with only a small delay and without sending information back to the cloud data centre. This requirement will be fulfilled by the development of hardware sensors with integrated computational processing power provided by a graphical processing unit (Janakiram MSV, 2019).

B.8 Software needs

In order to create seamless multiple system integrations, there will be a need for multi-system interoperability and software that can make sense of data. This could allow algorithms to predict a heart attack based on subtle changes in patient data recorded by home health monitors, or software to predict when a piece of industrial equipment requires maintenance before it fails. However, predictive analytics has not yet progressed to the point where it can be easily applied in every case, and this is one reason why a majority of data goes unused. Development and refinement of these algorithms is still largely yet to be done, and the skills and capabilities to conduct this work are in short supply (Manyika et al., 2015).

Critical security vulnerabilities are discovered frequently in operating systems and device firmware, requiring software updates to be installed. However, IoT devices may be inaccessible to software suppliers after deployment, leaving them vulnerable. Alternatively, leaving devices open to software suppliers may itself compromise security, given that software update mechanisms are themselves liable to attack. Many IoT devices will be unattended, with no means for devices to seek confirmation from their owners about when to deploy updates. Given the difficulties in deploying and updating software and firmware on many IoT devices, there may be growing willingness to investigate mechanically verified software.

B.9 Transmission and core networks

B.9.1 Cloud architecture

In order to support various IoT services, the NB-IoT and LTE-M will continue evolving as part of 5G specifications. The NB-IoT and LTE-M provide IoT services with low cost, long battery life, large coverage and high capacity support. Conversely, the 5G cellular system adopts software-defined networking and network function virtualisation for its underlying physical infrastructure, which 'cloudifies' access, transmission and core networks. The cloud structure of the 5G system separates user plane and control plane, allowing the operator to generate flexible network slices to fulfil the requirements of different IoT applications (Huawei Technologies Co. Ltd., 2016). Due to the vast connectivity, low latency and high reliability provided by 5G, expert telecommunications contributors to this report foresee that in the near future (e.g. two to five years), the cloud architecture of 5G, with the existing NB-IoT and LTE-M technologies, is likely to dominate IoT services.

B.9.2 Data transfer: adding fog architecture to the cloud

Over time, cloud technology has helped homogenise computing infrastructure (with notable exceptions emerging in general-purpose graphics processing units, field-programmable gate arrays and machine learning accelerated cloud infrastructure). The IoT will reverse this trend, forcing significant heterogeneity back into deployed devices—a consequence of the many and varied roles and deployment environments of IoT devices. Effort will be needed to support interoperation within the IoT ecosystem at many levels of technology (Desai et al., 2015).

Sending data to the cloud can require excessively high bandwidth and high energy costs. The large amounts of information transfer needed for the IoT will not be fulfilled by the existing cloud structure. Industrial control systems require very low latency (within a few milliseconds), and CAVs require a large network bandwidth (estimated to reach 1Gbps for each vehicle). These stringent requirements fall outside the current cloud architecture of 5G.

However, it is often unnecessary to deliver all the data to the cloud; approximately 90 percent of data can be stored and processed locally (Chiang and Zhang, 2016). The concept of 'fog architecture' has been recently proposed to serve functions such as computing, storage, control and networking distributed at the edge of IoT networks. Fog architecture allows efficiency, agility and low latency, and can bypass the need to send large amounts of data to the cloud (Chiang and Zhang, 2016). It will foreseeably rise to dominance in the next 10 years.

To enable fog architecture, the current transmission and core networks need to be altered from a centralised to a distributed architecture. Small data centres will also be required at the edge of IoT networks.

There are several opportunities in the development of fog architecture for transmission and core networks. Australian universities have research strengths in both information technology and communication, which provides a fundamental resource for R&D. Further innovation in the IoT space cannot be realised without fundamental infrastructure, such as fog architecture. Economic and commercial opportunities are likely to be generated in developing IoT infrastructure.

However, there are also many challenges. There are currently no off-the-shelf edge devices for fog architecture, but these will need to be more powerful and diverse than the existing network devices for cloud architecture. Further, the fog interface will need to be well-defined and compatible with existing cloud architecture. Security is another challenge in the development of fog architecture, as distributed systems are more vulnerable to attacks than centralised systems.

The future of IoT networking will see different application scenarios with various demands in terms of data rates, latency, reliability, transmission range, power consumption, cost and quality of service requirements. As such, multiple communication technologies will be applied in the IoT. Currently, LoRa and NB-IoT are competing for the LPWAN and may replace Zigbee or Bluetooth to some extent. At the same time, WiFi and LTE can support applications requiring high data rates.

B.10 Satellite technology

There is continuing growth in the delivery of satellite communication and in space science services. Satellite broadband high throughput systems are fuelling demand for spectrum arrangements to support ubiquitous earth stations for user terminals. Current Australian spectrum allocations to satellite services provide 1.55 GHz total uplink/downlink spectrum in Ku-band and 2.6 GHz in Ka-band. This is sufficient to support provision of broadband HTS at present. To meet the future growth in satellite broadband high throughput systems, ACMA is investigating possible additional allocations. In the Ku-band, sharing of the 10.7–11.7 GHz band with terrestrial fixed links is under consideration and could provide additional satellite downlink spectrum, while in the Ka-band, the range 27.5–29.5 GHz could provide additional satellite uplink spectrum. IoT networks are usually heavily biased towards uplinking more data than downlinking and can therefore be efficiently accommodated in the spare uplink capacity. In addition, IoT applications typically require only a small data-rate, and so a small section of spectrum can service a large number of sensors.

B.10.1 Low-earth orbit satellite constellations

In situations of disaster, emergency or defence, there may be a requirement for communication and internet services that can be integrated with terrestrial LTE or 5G networks to rapidly provide 100–200 km radius hotspots. Emerging technologies such as HAPS, stratospheric drones and stratospheric balloons could assist for these applications.

LEO satellite constellations can provide critical infrastructure to support IoT services, particularly for remote areas (e.g. agriculture, resources, ocean, forest) and moving objects (e.g. cars, boats, planes), where access to a terrestrial fixed wireless network is not available.

For remote areas and moving objects, LEO satellite constellations offer the advantages of global coverage, low signal delay times (quantified by the return trip time), low signal loss and low cost when compared to traditional geostationary earth orbit satellite systems. This allows satellite IoT terminals to be small in size and have a long life and low power consumption (Qu et al., 2017).

B.10.1.1 Emerging infrastructure in LEO satellite constellations

Examples of emerging infrastructure in LEO satellites include:

- The Iridium NEXT constellation of 66 satellites (completed in February 2019) will provide broadband, the IoT and hosted payloads services. The constellation has pole-to-pole coverage of the world, comprising six polar orbiting planes, each containing 11 crosslinked satellites, which create a web of coverage around the Earth (Iridum, 2019). The constellation, together with a small-form-factor transceiver known as the Iridium Certus^{SM} 9770, enables consumer and industrial applications that are portable and IoT-friendly, optimised for small size and low cost, with higher speeds than in the past.
- As of June 2020, SpaceX has launched 538 operational satellites of the planned Starlink constellation (Etherington, 2020). SpaceX has applied for licence approval to launch 4409 satellites, followed by another 7518, which will eventually form the full Starlink constellation. It is understood the spacecraft will fly in a relatively low orbit above the planet and beam internet coverage to the ground providing service to all areas of the globe. The constellation is designed to provide coverage to rural and remote areas, as well as provide another internet service option to customers. SpaceX intends to initially target the high-end gaming market.
- Australian-based start-up Myriota has IoT data terminals that connect directly to a constellation of proprietary nanosatellites, which have been trialled for water tank monitoring and defence applications. The company currently has four satellites in orbit and aims to build a constellation of 50 nanosatellites.
- Australian-based start-up Fleet Space Technologies has IoT data terminals which will be linked to a planned constellation of nanosatellites. In the Fleet system design, the IoT sensor and devices link to a terrestrial base station and the base station connects to the satellite. Fleet has launched its first satellites and is trialling application of its technology in the agricultural market.

B.10.2 High-altitude pseudo satellites and stratospheric drones

In addition to LEO satellite constellations, new technologies are emerging which can sit at even lower altitude than LEO satellites and provide LTE and 5G telecommunications base stations over fixed locations and payloads for earth observation surveillance. This includes HAPS and stratospheric drones.

B.10.2.1 Emerging technology from HAPS and stratospheric drones

Emerging technologies that sit at lower altitudes than LEO satellites, including HAPS or stratospheric drones, operate at around 20–25 km altitude in the stratosphere. The stratosphere offers a lower wind environment and is well known to have predictable and steady currents above northern Australia.

The advantages of HAPS include seamless interaction with terrestrial 5G and LTE networks and rapid deployment of a communication cell with a 125–200 km diameter.

Examples of emerging technologies include:

- Australia is home to Airbus' first global launch and retrieval site for its Zephyr HAPS in Wyndham, WA. The site was chosen due to the stable and predictable stratospheric currents (Figure 17).[34]
- SoftBank subsidiary HapsMobile, a joint venture established in 2017 by SoftBank and US aerospace company AeroVironment, is developing a HAPS called HAWK30, which can provide LTE and 5G services over 200 m in diameter (Figure 18). The Hawk30 is 78 m long, with solar panels and 10 propellers mounted to its wings. It flies above 20 km at around 110 km/h, with a flying time of several months.

B.10.2.2 Emerging technology for high-altitude balloons

Loon, an Alphabet subsidiary that arose out of Google, is developing stratospheric balloons which travel at around 20 km altitude in the stratosphere and provide LTE communications on the ground for internet connectivity. The balloon uses predictive models of stratospheric winds to rise and fall, taking advantage of different wind speeds and directions. Loon has tested its technology in Australia.

Figure 17: Airbus Zephyr Drone

Figure 18: HapsMobile's Hawk30 High Altitude Pseudo Satellite

[34] Airbus information provided publicly at the opening of the Wyndham, WA, launch and retrieval site.

B.10.3 Future enabling and emerging satellite technology

Over the next two to five years, the industrialisation of the LEO satellite sector is likely to produce the constellations of satellites necessary to provide internet and sensor network connections; these will provide critical communications infrastructure to enable the IoT. HAPS and stratospheric drones could allow LTE and 5G services to be established over disaster zones and remote locations. Improvements in battery storage and solar power systems could extend the current flight duration of 25–30 days to 100–120 days, allowing several HAPS or drones to provide annual coverage.

B.11 Future energy consumption

Many factors will influence how much energy will be consumed by the IoT. While it is difficult to make accurate predictions, a few general observations can be made. This analysis is divided into three main components:

- the IoT devices that collect data and carry out actions
- the communications infrastructure that manages information flow between the devices and data centres, where the data is processed
- the data centres where data are housed.

There are many factors that will influence how much energy the IoT will consume. With careful design, it will be possible to minimise energy consumption.

B.11.1 Devices

The energy consumption of IoT devices depends on factors such as the complexity of the computations the device performs for sensing and actuating functions, the ratio of the time it spends actively performing tasks to the time it is inactive, and the amount of data it sends and receives. In many devices, energy consumption is dominated by the process of communicating data to and from the device, either by wired connections or by wireless technologies (Gray et al., 2015). Wireless connections typically consume more energy than wired connections, as a transmitted radio signal is spread over a wide area and most energy is lost. It is likely that IoT communications will be predominately wireless due to a high number of widely dispersed and connected devices.

For devices in factories, offices and homes, power will typically be obtained via the conventional power network. Devices located away from conventional power sources may require the use of batteries. This approach has obvious undesirable environmental implications: even if a battery lasts for a year or more, the number of batteries to be disposed of each year on a global scale could become enormous. There is also a practical limitation on the ability to manually replace many batteries. For low-energy IoT devices, energy scavenging from the environment is an attractive option (Adila et al., 2018). Examples of energy scavenging techniques include light to electricity conversion (i.e. miniature solar cells), vibrational or other forms of energy gathering from motion or ambient sound, and scavenging ambient radio frequency energy from radio and TV stations.

B.11.2 Communications infrastructure

The structure of the communications component of the IoT will be like the conventional internet. However, a key difference is that the communications backbone of the IoT needs to provide access to many more devices than the internet, and these devices are often in places where the conventional internet may be less accessible. The energy consumption in many IoT devices is dominated by the energy required for communications. Likewise, the energy consumption in these systems will be highest in communications infrastructure closest to the IoT devices (Tahiliani and Dizalwar, 2018), as it is necessary to provide access nodes near all IoT devices. As the number of IoT devices increases, so too does the number of access nodes, and therefore the total energy consumption.[35] However, as data is aggregated further into the network (away from the IoT devices), the communications infrastructure is shared between many devices, and energy efficiencies are likely to result from economies of scale.

Data centres

While the nature of the data in the IoT will be different, it is likely that data centres in the IoT will also dominate energy consumption for this technology, like the conventional internet. IoT devices can increase indirect energy consumption through the use of live-streaming and internet-enabled capabilities that depend on remote data centres (Morley et al., 2018). While many (but not all) data centres have committed to 100 percent renewable energy targets, current demand for data is growing at a faster rate than can be met by renewable supplies (Cook et al., 2017). Data centres currently consume more than 400 terawatt hours of electricity per annum (Whitehead et al., 2014), which, together with other internet use, represents about 10 percent of the global electricity usage (Andrae and Corcoran, 2013).

One factor that will affect data centre energy consumption is the location of the data processing. Centralised or 'cloud' processing is efficient because the equipment is shared, but centralised processing requires more energy-consuming transmission infrastructure. Distributed processing (also referred to as fog or edge processing) in which the data is processed in smaller processing units closer to the IoT devices could provide efficiency gains (Jalali et al., 2016).

[35] For systems that are node-based, such as terrestrial cellular IoT systems.

APPENDIX C SECURITY

C.1 Security attacks in IoT systems

IoT attacks can be categorised into five areas:

- communications
- devices/services
- users
- mobility
- integration of resources.

C.1.1 Communications

Attacks on IoT communications can be broadly categorised into routing attacks, active data attacks, passive data attacks and flooding attacks.

In a routing attack, attackers target routing protocols and network traffic to either disrupt the flow of information or redirect the routing path to an unsecure destination. They neither alter the contents of, nor attempt to gain information from, the transmitted packets. Common forms of these attacks include blackhole, wormhole and pharming.

Active data attacks alter or delete information by targeting valid data packets directly rather than via subverting network routing. Examples of these attacks include channel jamming and various forms of data tampering (modification, manipulation etc.), which may or may not result in valid packets. Active data attacks may target the packet payload, header or both.

Passive data attacks attempt to gain information without altering the contents of communications. Examples include eavesdropping and traffic analysis.

Examples of flooding attacks include SYN flooding and denial of service attacks, where a succession of requests are sent to consume server resources to make a system unresponsive to legitimate traffic. Denial of service attacks are of particular concern for IoT systems due to the resource-constrained nature of many IoT devices. It may only take a limited amount of bogus traffic before an IoT device is compromised by resource and bandwidth consumption.

C.1.2 Devices and services

Threats on the devices and services of an IoT system can be broadly categorised into physical attacks, device subversion attack, device data access and device degradation. The vast majority of IoT devices operate in open environments, where common security issues include device damage and disconnection. For instance, an attacker can physically disconnect an IoT device, damage it beyond the point of serviceability or even destroy it completely.

In a device subversion attack, an attacker assumes full or partial control over a device. This can then be used to actively cause the device to either cease functioning or to provide incorrect outputs. Taking control of IoT devices can be divided into two categories: controlling a single device and controlling many devices. This can lead to the device's functionality being unavailable, restricted or misused. The low power of IoT devices makes them more vulnerable, due in part to the minimal (or non-existent) security protections that are embedded in such devices. Moreover, these devices are often incapable of updating to the latest software and security patches, even when they have embedded security functionality.

In a device data access attack, an attacker infects one or more IoT devices, which are then used by the attackers to perform malevolent activities on sensitive data without the user's knowledge. The device appears to be functioning normally, but the data held by the device is available to the attacker.

Device degradation is a form of denial of service attack intended to prevent access to a service by attacking the functioning of the devices themselves, rather than the network's ability to handle traffic. In a typical denial of service attack, the service is overwhelmed by having to process bogus traffic but the individual nodes are unharmed. With their limited memory space and battery capacity, IoT devices can be attacked by memory exhaustion and battery corruption. Thus, a mass-scale device degradation attack on these resource-constrained devices could potentially collapse the entire system's operations.

C.1.3 Users

Potential security attacks associated with users can be divided into four broad categories: trust, data confidentiality, identity management and behavioural threats.

The scale of the IoT means that trust is an even more pressing issue than is traditionally the case. Interactions may be fleeting, and devices will interact with a large number of unknown devices. Trust-related attacks include self-promoting (a malicious device providing good recommendation for itself), bad mouthing (an attacker providing bad recommendation against a good device) and good mouthing (bad devices providing good recommendations for other compromised devices) attacks.

The potential utility of the IoT lies in the richness of the data that it contains. This may include extremely sensitive user data, such as age, address and health records. A user's privacy can be breached by any attack that accesses that personal information. Attackers may manipulate or disclose such data or use it to impersonate the user.

User impersonation in the IoT is a critical issue due to the combination of heterogeneous data sources coming from various IoT devices, contexts and locations. This can be done via identity spoofing, where attackers gain unauthorised access to IoT systems. With the IoT's scale and heterogeneity and users' desire for privacy, it is likely that users will maintain multiple identities. This also multiplies the normal vulnerabilities that attackers can exploit, due to the range of interactions of the systems supporting these identities.

Management of identities is a major concern for authenticating and authorising a legitimate device, especially when the service provider and the service consumer both try to keep their identities hidden. Attackers may exploit the heterogeneous and multi-domain nature of the systems supporting identity management in the IoT to subvert these systems.

In personal and social domains, users' malicious or selfish behaviours can also be used to create attacks through social engineering, such as being tricked into revealing private information through phishing attacks or downloading malicious software.

C.1.4 Mobility

The various mobility-related security issues can be divided into three categories: dynamic topology/infrastructure, tracking and location privacy, and multiple jurisdictions.

Some threats can be viewed from multiple perspectives. For example, users' mobility may increase the possibility of active and passive data attacks (communications) and location tracking (mobility). In the IoT, nodes do not necessarily need to connect over the internet; they can connect via any network. In such an environment, when users and devices move (i.e. joining and leaving the network), the network topology is dynamically modified. This could generate security challenges of interdependencies (e.g. attacks on networked cars, electronic medical devices and power stations) for end-users. This could further evolve into a 'sinkhole' attack if attackers update the network topology and gain illegal access to a user's data in real time.

In the context of tracking and location privacy, location-based information (such as a user's current position or daily routine) in an IoT system could be inherently vulnerable and a possible target for a personal privacy breach. Attackers may seek to exploit any mismatch in policy settings, identity management or security technologies. For instance, in a traffic accident, police officers can communicate with emergency services regarding the status of a driver or passengers. However, the management of this information across jurisdictions is a challenge for data privacy.

C.1.5 Integration of resources

In IoT systems, from data collection to data processing, storage and usage are highly dependent on diverse infrastructures. Attacks in this area can be divided into three broad categories: cross-domain administration, cascading resources and interoperability.

The components which co-operate and interact to provide end-user results may be controlled by multiple different domains. Even when control resides within a single domain, there are security challenges at each stage of the structure. In such cases, attackers may seek to exploit any mismatch in policy settings, identity management or security technologies.

End-user applications in IoT systems can potentially draw upon a vast range of devices and services. Any low-level security breach may cascade up and affect higher-level services and applications that depend on the compromised component. For instance, an attacker can penetrate a user's mobile network and make a modification to their home automation system and compromise a motion sensor. If the system is set to open windows or doors when motion is detected, the attacker may be able to gain access to the building. Furthermore, the large volume of data can create threats to the user's privacy and information security. Such attacks allow an attacker to gather a large amount of information (of service, user and resources) and perform automated datamining without being noticed by the user or service provider.

Interoperability relates to attacks based on the need for multiple systems to work together and the ability of attackers to exploit any potential issues. Interoperability in an IoT system can include cloud computing, fog computing, social networks, mobile computing and industrial networks. For instance, a smart healthcare system requires collection, analysis and transferring of information (e.g. blood pressure) to patients by healthcare professionals, which may depend upon several of these dynamic networks. Therefore, at any of these stages, attackers can breach patient's personal (and sensitive) information by penetrating any of the networks between the infrastructures.

C.1.6 Increased risk of national security threats

Greater cooperation with foreign companies in global supply chains has raised concerns about the emergence of increased national cybersecurity threats. While this is not exclusive to the IoT, Australia is exposed to cybersecurity risk through the high proportion of overseas stakeholders who will likely develop and provide IoT systems. Care should be taken when sourcing IoT devices or components from countries with poor security and privacy track records. However, there is an opportunity for Australian companies to show leadership by creating niche hardware and software products domestically that could reduce our reliance on buying end-to end components from countries with poor previous performance in security and privacy management.

C.2 Mitigating risk

Securing IoT systems requires efficient attack prevention and detection, as well as measures for the containment and recovery from attacks. Although the security techniques that can be deployed to mitigate the attacks fall under the traditional categories of authentication, authorisation, secure communication and trust management, these techniques need to be addressed within the specific context of the IoT and integrated with different services and protocols in the IoT architecture.

C.2.1 Device identity, authentication and monitoring

Identifying and authenticating devices is a practical and security challenge for the IoT. Device identity is important when it comes to establishing who can access a device and what that device can connect to. Access to devices by 'authorised' users is necessary:

- **at the time of setup, when connectivity rules are established:** there is a practical challenge about how to achieve authentication of IoT devices in an efficient manner, as the devices are computationally constrained. Authentication would need to occur at a large scale when IoT systems use thousands of devices and sensors. Mass devices may also need secure registration, which requires protocols for secure provisioning of IoT devices.
- **on an ongoing basis:** access is needed to authorise security and tech upgrades. Assessing a device's security framework is also dependent on its behaviour over a period of time. It is necessary to take into account both static and dynamic characteristics of a device in making this assessment.
- **at times of crisis:** for detecting which device has become malicious or exposed a system to attack, and also to provide fixes (e.g. security software and patches). This may be especially difficult if the devices are consumer owned.

C.2.2 Secure authorisation and management

The main challenge in the design of secure authorisation services in IoT systems arises due the different jurisdictions the IoT devices cover and their respective security policies.

For instance, it is not realistic to assume that the identities of all users who need access will be 'known' beforehand (i.e. a retail shop may not know the identities of its customers until they walk through the door). Therefore, the design of authorisation services in IoT systems need not only to be lightweight but also to have the flexibility to deal with dynamic situations. They also require fine-grained policy decision capabilities and a decentralised architecture for real-time decision making to achieve the desired performance.

C.2.3 Trust mechanisms

The credibility and reputation of devices is key to ensuring accurate and reliable network service delivery. Each system will need to determine what device functionalities are required to accept the device and how trust should be evaluated and managed in distributed IoT structures over time. This will become even more important when devices and sensors are mobile, moving from one jurisdiction to another, or where they are not known in advance.

There are two classes of techniques (hard trust and soft trust) which can be used to achieve trust management. Hard trust techniques involve the use of mechanisms that monitor and evaluate the state of a device, thereby helping to assess whether a device has been compromised. Soft trust techniques involve the use of reputation mechanisms such as querying neighbouring IoT devices and gateways to assess and calculate a device's reputation based on direct observations of past actions and behaviour (Bica et al., 2019). These types of hard and soft trust mechanisms can generate suitable trust management schemes, especially for large, dynamic IoT systems.

C.2.4 Mitigating software and data security risks

While the preferred solution to dealing with software vulnerabilities is the application of patches, this requires a user to register their device with manufacturers, which may not always occur. IoT devices may not be designed to receive regular software updates, or users may forget unattended devices installed on their networks, leaving them with outdated software. Due to the small cost/profit margins associated with consumer devices, there may be limited incentive for manufacturers to provide the required software patches in a timely and regular manner. The security record of domestic IoT devices has been limited, particularly within consumer products such as whitegoods and internet-enabled toys. Given the difficulties in deploying and updating software and firmware in many IoT devices, there may be a growing willingness to investigate mechanically verified software, such as that used with the seL4 operating system microkernel and its derivatives (Klein et al., 2009).

Security is also required when data resides in an IoT device and when in transit over networks. Data security and information integrity must be supported by a trusted computing base. If IoT devices are designed not to be updated or recovered, their data should be deleted over time; encryption mechanisms lose their strength and are unlikely to remain secure over the long term. As IoT deployment increases over the next 10 years, guidelines, regulations and/or legislation may be required to ensure that IoT devices operate securely.

C.3 International solutions

Concerns about IoT security are not unique to Australia. Other jurisdictions are already grappling with these issues, and Australia will likely derive some benefit from their efforts to impose requirements on the physical design and security of IoT devices.

In the US, as of June 2020, the Cybersecurity Improvement Act is currently before Congress and aims to address physical security concerns relating to IoT devices.[36] The Security of Connected Devices legislation in California imposes similar restrictions, albeit at a state level only.[37] These legislative responses have, in part, been criticised for not appropriately balancing economic and security considerations (Ellis, 2019), and it is too early to assess their efficacy (for example, the Cybersecurity Improvement Act is not yet in effect). Additionally, non-binding technical standards for securing IoT devices have also been released in multiple jurisdictions (European Union Agency for Cybersecurity, 2020).[38]

The United States Department of Homeland Security has warned that malicious actors can 'inject, replay, modify and/or intercept' data from medical devices (Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, 2020).

The US Federal Trade Commission has brought a number of actions, including:

- in 2014 against SecurView. This baby monitor and security system allowed access to a video feed and audio remotely via a web interface or mobile application, but also transmitted login and password information in clear format. The system was hacked in 2012 and the feeds of 700 cameras were posted online.
- in 2017 against D-Link, alleging that the IP camera and router manufacturer did not meet reasonable security standards, resulting in customer vulnerability (no incident was reported).[39]

The choice between using mandatory (legislated) and voluntary (industry-driven) responses to mitigate concerns regarding the security of the IoT is complex. Any mandatory requirements imposed in Australia should therefore take a holistic and principles-based view. Co-regulatory approaches and legislative changes should be considered where appropriate.

[36] IoT Cybersecurity Improvement Act of 2019, S. 374, 116th Congress (2019).

[37] Security of Connected Devices Act, S. 327, California (2018).

[38] The European Union Agency for Cybersecurity has released a number of 'good practice' guides on IoT security.

[39] *Federal Trade Commission v. D-Link Corporation and D-Link Systems*, FTC Matter/File Number: 132 3157, https://www.ftc.gov/enforcement/cases-proceedings/132-3157/d-link. For a list of other vulnerable devices, see Vijay Sivaraman and others, *Inside job: security and privacy threats for smart-home IoT devices* (Australian Communications Consumer Action Network, 2017).

APPENDIX D
PRIVACY AND OTHER LEGAL ISSUES

D.1 Privacy and post-supply impacts on consumers

D.1.1 Increased data collection

As the use of IoT devices becomes more widespread, this increases the likelihood that a greater quantity of data – and data that is more intimate and personalised in quality – can, and will, be collected and processed. However, users' knowledge is often limited as to:

- *what* and *how much* data is being collected the *uses* of the data
- *who* is receiving the data
- *how long* that data will be used.

The developmental tendency of the design of many IoT devices towards reduced visibility can also affect this situation, to the detriment of the customer.

D.2 Australian privacy law and governance

In Australia, the Privacy Act and the associated APP apply to the handling, accessing and correcting of personal information. Most states and territories also have separate privacy legislation and frameworks that complement the national approach. Obligations consist of the handling of citizen data by public sector agencies, with higher thresholds for the use of health and workplace data (Australian Privacy Foundation, 2018; Office of the Australian Information Commissioner, 2019a).

Currently, the Privacy Act imposes obligations on 'APP entities', which include Australian Government entities, office holders or organisations (includes individuals, body corporates, partnerships, unincorporated associations or trusts), when dealing with personal information.

However, some exemptions apply, for example it does not extend to companies with an annual turnover of less than $3 million[40] or registered political parties. In addition to the Commonwealth Privacy Act, state and territory privacy legislation may also apply. Health services are also considered APP entities under the Privacy Act no matter the size of their organisation.

Under APP 11, an APP entity must take such steps as are reasonable in the circumstances to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure. Redress mechanisms that exist in the Privacy Act

[40] However, smaller companies may be bound by its provisions either under a Commonwealth Contract, and/or bound to the protections included in the EU's General Data Protection Regulation due to trading internationally in Europe, or have entered into other forms of privacy protection under contract law.

include the ability of an individual affected to complain to the OAIC; the notifiable data breaches scheme contained in Part VII of the Act, which requires entities to notify individuals of eligible data breaches; and the OAIC's ability to investigate matters on its own motion. In the case of serious and repeated breaches of privacy under the APPs, the APP entity may be subject to a civil penalty of up to 2,000 penalty units. Along with the ability to investigate complaints initiated by affected parties, the OAIC also has own-motion investigation powers where it suspects a breach of the Privacy Act or APPs has occurred.

Research considering the applicability of the APP in the Privacy Act has noted that 'the APPs have significant regulatory uncertainties or gaps when it comes to [IoT] privacy' (Mathews-Hunt, 2017) and that '[t]he APPs are too weak to meet [IoT] challenges and based upon current OAIC strategy and government under-resourcing, are unlikely to exert a positive influence over the promotion of privacy into the future' (Mathews-Hunt, 2017). Scholars examining Australian privacy legislation have concluded that the Privacy Act is 'incomplete and inadequate' in the context of the IoT (Manwaring, 2018; Richardson et al., 2016). These opinions are not confined to scholars; they are also supported by a small empirical study conducted by the University of Melbourne. Both users and developers of IoT products were surveyed in this study, and both sets of participants indicated significant uncertainty surrounding privacy regulation in Australia (Bosua et al., 2017). Specific limitations are listed below.

D.2.1 Consumer data and personal information

Many types of consumer data may not be subject to the Privacy Act, particularly if reasoning in a recent judicial interpretation of the meaning of 'personal information' is adopted more widely. In *Privacy Commissioner v Telstra Corp Ltd* [2017] FCAFC 4, journalist Ben Grubb sought access to metadata held by Telstra relating to his use of telecommunications services. Both the Administrative Appeals Tribunal[41] and the Full Federal Court[42] on appeal proposed a narrow construction of the meaning of personal information 'about an individual'. For example, the Full Federal Court considered that the colour of Grubb's mobile phone and his network type was not information 'about' Grubb, and therefore not personal information (*Privacy Commissioner v Telstra Corp Ltd*). Similarly, the Administrative Appeals Tribunal gave an example of car service records and stated that these would not constitute information 'about' the car's owner, even if the records contained the owner's name and the car's registration number (*Telstra Corp Ltd and Privacy Commissioner*; Yuvaraj, 2018). Significant uncertainty still remains as to the meaning of 'personal information' (Australian Competition and Consumer Commission, 2019a; Leonard, 2017). The definition of 'personal information' in the Privacy Act has been reworded since the decision in *Privacy Commissioner v Telstra*, but the rewording did not clarify the scope of information being 'about an individual'. If similar reasoning to the Full Federal Court and the Administrative Appeals Tribunal in the Telstra case is adopted by businesses, regulators and/or the judiciary,

[41] Telstra Corp Ltd and Privacy Commissioner [2015] AATA 991.

[42] Privacy Commissioner v Telstra.

much information of value to consumers and third parties collected, processed and/or disseminated by means of IoT devices may be treated as falling outside the protections of the Privacy Act. The ACCC has already recognised the uncertainty and potential under-inclusiveness of the definition in the context of digital platforms and recently recommended clarification of the definition of 'personal information' to include 'technical data' such as location data and online identifiers (Australian Competition and Consumer Commission, 2019a).

D.2.2 Enforcement constraints

Enforcement mechanisms do not provide a direct right of action for consumers. Although under section 36 of the Privacy Act consumers may make a 'complaint' to the regulator, few determinations have been made under this provision (Greenleaf, 2014), which has resulted in minimal appellate jurisprudential development. Historically, sanctions have been insubstantial. In the UK for example, no civil penalties (available up to AUD $2.1 million) have been awarded since their introduction in 2014 (Information Commissioner's Office, 2018).

D.2.3 Consent

Consent overrides most safeguards for consumers in relation to the use of consumer data and its transfer to third parties. The adequacy of consent to protect data subjects has been vigorously contested (Australian Law Reform Commission, 2008). Commercial entities are permitted to deal with consumer data even though in most cases the nominal consumer consent obtained is often not informed, is non-negotiable, and is subject to unilateral interpretation and extension by the commercial party. This problem is exacerbated by forms of consent and privacy policies that are often lengthy, difficult to understand, ambiguous, hard to find, or broad (Australian Competition and Consumer Commission, 2019a). Empirical evidence suggests this encourages consumers not to read most policies or to accept unfavourable terms because '[i]t [is] the only way to access the product or service' (Nguyen and Solomon, 2018).

D.3 Liability and blame

D.3.1 Identifying losses

The contractual arrangements within a network can make it difficult for end-customers (including enterprises) and network actors to identify all applicable contracts, let alone interpret them. It also becomes difficult to determine who should bear losses, and how the cause of loss can be identified and evidenced. Currently, most losses caused by IoT devices are borne by either the victim or the responsible entity in each case.

Losses can be borne by:

- those who suffer the loss in each case (e.g. the users whose data is compromised, or the businesses whose operations are affected by malfunctioning IoT devices)
- the responsible entities in each case, assuming they can be identified (such as traditional civil liability, where the one who commits the act is responsible for its consequences)
- the broad category of people who are likely to suffer loss (such as a compensation scheme that is funded by the users of IoT devices)
- the broad category of people who are likely to cause such losses (such as a compensation scheme that is funded by a tax on the manufacture or supply of IoT devices)

- an industry body (e.g. a compensation scheme funded by an IoT association)
- the state (such as a compensation scheme funded by the general treasury) (Calabresi, 1970).

Determining which of these 'loss' options is desirable in the context of the IoT is a question that can often only be answered on a case-by-case basis, with reference to specific social and moral contexts.

D.3.2 Allocating liability

IoT device ecosystems can also hamper the allocation of liability for faults. Where there are multiple providers, liability becomes uncertain. Defects in an IoT device ecosystem can arise in several places, including physical faults in the dominant object or embedded computer hardware, bugs in the software, corruption or deletion of data, or failure of network connections. An overall detriment may arise from a combination of defects, such as when a network failure corrupts data, causing the IoT device to fail to recognise critical inputs. This presents significant issues for both customers and the law.

D.3.3 Enforcing liability

Addressing and resolving liability raised by the IoT has been described as a 'legal feeding frenzy' (O'Donnell, 2018). Even where liability is clear, the mobile nature of IoT devices and the differing locations of provider network actors can make practical enforcement difficult. Australian customers are particularly affected, as most IoT devices they purchase are imported, with contracts likely to contain foreign jurisdiction and foreign law clauses. Contract drafters for provider networks also inevitably attempt to avoid liability, using favourable jurisdiction and choice of law clauses, or arbitration and class action waivers – practices already common in conventional e-commerce. These impediments, combined with the usually low value of a customer claim relative to legal costs, often hinder customers achieving redress.

For defective goods claims brought under the Australian Consumer Law, an action may be successfully defended by establishing that the state of scientific or technical knowledge at the time when the goods were supplied was not such to enable the relevant defect to be discovered.[43] This 'start of the art' defence is rarely relied upon in Australia.[44] Notably, a 'small statistical chance of injury' associated with a given product does not in itself mean that it is defective.[45] While most commentary on this defence is grounded in a pharmaceutical context (Tsui, 2013), it may prove useful in cases concerning the IoT. Simply because an IoT device gives rise to some inherent small and statistical chance of injury should not necessarily imply that it is defective. Such a risk may be accepted where the economic benefit is sufficiently high.

All of these uncertainties are likely to obstruct proper redress for both public and private sector customers, particularly in relation to low-value contracts. However, customers are not the only ones facing detrimental effects. Uncertainty about the

[43] *Competition and Consumer Act 2010* (Cth) sch 2, s 142(c).

[44] There have been only two prominent cases dealing with the state of the art defence in Australia. See *Graham Barclay Oysters Pty Ltd v Ryan* [2000] FCA 109 and *Peterson* v *Merck Sharpe & Dohme (Australia) Pty Ltd* [2010] FCA 180. In both cases it was found that the state of the art defence was available to the defendant.

[45] Such a view has been found in the Explanatory Memorandum, Trade Practices Amendment Bill 1992 (Cth), 8 cited in Tsui (2013).

legal liability of provider network actors may hinder investment and innovation in IoT devices. Recent research by the European Commission's Expert Group considered liability for emerging technologies including the IoT (Expert Group on Liability and New Technologies – New Technologies Formation, 2019). Their key findings included:

- it may be appropriate to impose strict liability (liability without any finding of fault) for damage caused by emerging technologies in limited situations (such as the use of drones or autonomous cars in public spaces)
- the burden of proof for causation and damage is generally on the victim, but in limited circumstances, it may be appropriate to reverse or lower this burden, particularly where such a burden would be disproportionality high or if damage was caused by a breach of some other set of rules (such as rules on information security)
- where multiple people or companies cooperate to provide different elements of some technology, they should be jointly or severally liable for harms caused by that system
- insurance may need to be mandatory for certain technologies if the potential harm is more frequent or more severe, or if operators are unable to provide redress to individuals (such as start-ups with limited capital for redress).

D.4 Other legal considerations

Potential or actual issues related to the IoT in Australia have been identified in a number of legal areas. These have largely been in the context of protecting citizens, consumers and businesses against the risks outlined earlier in this report. These areas include:

- data protection and privacy (particularly in the Privacy Act) (Manwaring, 2017b; Mathews-Hunt, 2017)
- consumer protection (particularly in the Australian Consumer Law), and common law and equitable principles governing business-to-consumer contracts, especially consumer guarantees and product liability (Manwaring, 2017b), misleading and deceptive conduct and false representations, unconscionable conduct (Manwaring, 2018), and unfair contract terms (Mathews-Hunt, 2017)
- criminal prohibitions and enforcement in relation to cyberattacks (particularly in relation to the criminal codes in each state, territory and federally) (Manwaring, 2017b)
- intellectual property (particularly the *Copyright Act* and its interaction with contract and licensing law), such as restrictions on software or digital content contained on a device, or where a consumer may want to make repairs or software modifications to their device (Manwaring, 2017a)
- dataveillance of citizens by the state and of consumers by corporate interests (Clarke and Greenleaf, 2017)
- Competition law (*Competition and Consumer Act 2010* (Cth)), concerning the governance of the emerging roaming services market, where roaming mobile devices and sensors may cross over network boundaries (Halliday and Lam, 2015)
- spectrum allocation (Halliday and Lam, 2015)

- product liability law and insurance law (particularly relating to CAVs and other machines with autonomous decision-making capabilities) (Halliday and Lam, 2016)
- ethics (for example, in autonomous decision making) (Manwaring, 2017b)
- network neutrality and whether some data flows should be prioritised over others (such as health data), where there is the risk of network congestion (Halliday and Lam, 2015)
- discrimination (Australian Competition and Consumer Commission, 2019a, p. 517)
- the definition of 'goods' in sale of goods legislation and other legislation (Mathews-Hunt, 2017)
- retention of metadata (Halliday and Lam, 2016)
- fairness and validity of private enforcement of legal rights through remote disablement and similar provider control mechanisms (Manwaring, 2017a)
- liability allocation and enforcement issues against providers due to privity of contract and the use of subsidiaries with limited equity as contracting parties (Manwaring and Clarke, 2015)
- validity of evidence derived from IoT devices in investigations and litigation (Laykin, 2017).

As yet, there are no IoT-specific legal rules that apply in Australia and very few in other jurisdictions. This is not to say that the IoT is not regulated. There exists a substantial amount of legislation general enough in application, and sufficiently adaptable common law and equitable principles, to apply to a variety of new products, activities and relationships brought about by IoT devices (Brownsword, 2008; Manwaring, 2017b, 2018).

D.4.1 Hacking

Although 'hacking' (unauthorised remote intrusion) is already a criminal offence, technologically specific drafting may mean that criminal legislation may be insufficient (Manwaring, 2017b). Many IoT devices (particularly inexpensive ones) are *not* password-protected, and the buyer (customer, business or public sector) usually has no capacity to implement password protection for themselves, due to product and system design (Manwaring, 2017b). Furthermore, even when rules do cover all relevant conduct, they are ineffective if they cannot be enforced. While a hacker may be in breach of a 'no access without lawful excuse' rule, it is difficult to enforce criminal penalties if they are undiscoverable or located out of the jurisdiction (Manwaring, 2017b).

D.4.2 International actors and national security risks

The complexity of modern hardware supply chains, the lack of significant domestic IoT manufacturing activity, and the cost advantages enjoyed by most overseas IoT device manufacturers have made Australian users heavily reliant on IoT devices that are, at least in part, manufactured or assembled offshore.

This can present a national security risk. The extent to which Australian regulators are equipped to assess or oversee the physical security risks associated with such IoT devices is unclear, and the burden on Australian security personnel to vet such devices is increasing (Walsh and Pan, 2018). Even where IoT devices are functioning as intended and are not faulty *per se*, misunderstandings about features or inadequate guidelines for their use can nonetheless give rise to security vulnerabilities if insufficient consideration goes into their deployment.

For example, in 2018 the IoT fitness device company Strava published three trillion points of location data from its 'global network of athletes' (Strava, 2019). Intended to allow Strava users to 'discover new places to be active,' (Strava, 2019) the feature unintentionally tracked and publicly shared the movements of military personnel in confidential locations (Bogle, 2018). The leak was described as an 'open source intelligence gold mine' (Bogle, 2018).

D.4.3 Evidentiary value of IoT data in courts

The prudent use of IoT devices may be to reduce the probability of a dispute occurring, or to more easily settle or determine claims when disputes do arise. While not yet common in Australia, the use of IoT device data as evidence is already occurring overseas (Katz et al., 2017). The evidentiary and policy considerations relating to the use of IoT device-generated data in legal proceedings are significant.

IoT devices are designed to passively collect data on an ongoing basis (Manyika et al., 2015). The extent to which this data can be requested by criminal law enforcement, or plaintiffs in civil proceedings, needs to be carefully managed. Records from IoT smart home devices have already been requested in international court proceedings (Hearn, 2018). 'Fishing expeditions' – where IoT device data is requested solely on the basis that the IoT data may or may not have evidentiary value – will need to be carefully monitored.

Simply being aware that a criminal act or civil contravention occurred in a specific venue may (or may not) be of sufficient probative value for access to the data collected by nearby IoT devices to be granted. A case-by-case analysis will be required.

D.4.4 Impacts of poor or autonomous decision making

The risks of poor autonomous decision making have been discussed in the ACOLA report, *The effective and ethical deployment of artificial intelligence: An opportunity to improve our wellbeing* (Walsh et al., 2019). In the context of the IoT, although the risks are not new, the increased prevalence of autonomous IoT devices can increase the likelihood of such incidents occurring.

All IoT devices can collect, handle and communicate data. However, data may be or become inaccurate during the IoT device's performance of any of these processes. Sensors can be misled by physical phenomena, algorithms can be wrong and data records can be corrupted.

Customers, the provider network and others who rely on accurate data are at risk of harm if the data is inaccurate. This is particularly the case where the IoT device has autonomous decision-making capabilities; decisions may be made for the user without adequate notification and/or capacity for manual override.

Even when data is accurate, IoT devices with some autonomous decision-making capability are risky. The existence of autonomous decision making also raises a fundamental question of liability: who should be liable for harm caused by a machine, or an unfavourable and unwanted contract entered into by a machine, which was not foreseeable by the machine's user (or its programmer)? The application by judges of private law principles (such as in contract and tort) will mean that liability will be allocated in some form, but it may not meet societal expectations on accountability.

Where IoT data are used in decision-making algorithms in government, in addition to liability in contract and tort, protections for the public in anti-discrimination and administrative law will apply. For example, the rule against bias in administrative law will put government under a certain obligation to ensure that their use of IoT data in automated decision making is free from any bias, even if this exists in the data already. To combat this, it may include use of human oversight or explainable algorithms to spot potential bias.

D.4.5 Data-based discrimination

The IoT promises data-driven decision making and personalised access to services. Data can be used to decide whether to offer particular products or services, or to vary the conditions on which those products or services are offered, according to the attributes of individual consumers.

Data-based discrimination can be deliberate or unintended. Inferences drawn from data are often difficult to perceive because machine learning algorithms are opaque. Further, providers may deliberately conceal the reasoning behind their decisions. Providers may also rely on a network of third-party products or services that are not transparent with data-collection practices.

One area of particular concern is 'algorithmic discrimination', where the often relatively small and/or selective datasets used in machine learning contain societal biases. There is a significant emerging body of research describing algorithmic discrimination on the basis of data collected on race, gender, health status and socioeconomic status (among others), and its effects on areas such as employment opportunities, housing, policing and sentencing policies.

Some forms of data-based discrimination are already unlawful in many jurisdictions, such as refusing to supply goods or services, or supplying them on less favourable terms. Australia's anti-discrimination law framework would apply to many decisions made that take IoT data into account. Anti-discrimination law also protects against indirect discrimination, where a policy or approach that is equally applied has a discriminatory effect on a particular group. As anti-discrimination law is not technology-specific, it should not matter if the discrimination has its base in data (neither is this likely to be a defence if the data itself is biased). For example, the *Disability Discrimination Act 1992* (Cth) applies to decisions that are made in the course of employment, education, access to public premises, and provision of goods and service amongst others. However, other forms of discriminatory conduct, such as price discrimination (Australian Competition and Consumer Commission, 2019a, p. 517) based on data provision conditions, can be engaged in without legal restrictions. The possibility that fundamental human rights can be undermined by both lawful and unlawful discriminatory conduct is real and urgent.

APPENDIX E
OTHER SOCIAL CONSIDERATIONS

E.1 Psychological impacts of IoT technology on the individual

Technology-specific impacts can be difficult to disentangle from broader social and cultural shifts. As a result, there are significant challenges of causal attribution. Substantial caution is required when considering potential psychological impacts on individuals arising from the spread of IoT technologies. The following issues are most often identified by expert opinion and are consistent with trends observed in existing technologies.

E.1.1 Positive and negative psychological consequences

There are likely to be both positive and negative psychological consequences arising from changing, IoT-mediated opportunities to fulfil the basic human need for social connection. Evidence from social media research suggests the following:

- Social IoT technology will not *cause* people to be happier or more distressed. Rather, it will tend to amplify existing psychological characteristics and risks (Ryan et al., 2017). Those who rely on casual interactions for most of their interpersonal interactions may be particularly at risk from growing IoT-enabled automation in public spaces.
- Social IoT technology that perpetuates the development of online-only (or perhaps bot-driven) relationships may drive negative impacts, such as social isolation and withdrawal, since these relationships ultimately cannot satisfy social connectedness needs in the real world (Ryan et al., 2017). For example, amongst isolated and/or lonely older adults, greater ICT use predicts poorer psychological adjustment (Fang et al., 2019).
- A greater visibility of performative social displays (such as IoT-enabled social interactions in smart urban settings) has the potential to drive negative psychological impacts, such as loneliness, in those who feel excluded or disenfranchised from such interactions.
- Social IoT technology will *not* fundamentally change the nature or size of social networks in terms of the most valued relationships (Dunbar, 2016). Mental health-relevant interactions, such as support in times of significant distress, will continue to rely on interactions amongst a small network of highly trusted friends or family. Digital technologies may create new channels for these interactions but will probably not alter their nature.

E.1.2 Potential consequences arising from a reduction in 'socially useful ambiguity'

Humans regularly and routinely provide incomplete or inaccurate accounts of their behaviour and motivations for the purposes of navigating social relationships, even with close ties. These partial truths and 'white lies' fulfil important social functions (Iniguez et al., 2014) to manage others' perceptions of ourselves, protect others from hurt or harm, and enable personal autonomy.

A growth in sensor-equipped smart infrastructure in urban, home and workplace settings has the potential to erode this socially useful ambiguity if information about location, behaviour and social interactions becomes available to employers, government and social peers. IoT data itself may be amenable to ambiguous interpretations, increasing scope for disagreement. Impacts include:

- acute negative psychological effects such as direct social conflict when ambiguity is eroded (the parents who can now directly monitor their teenager's location)
- insidious negative consequences such as depression (Kim et al., 2012) associated with erosion of interpersonal trust driven by societal or workplace cultures in which individuals can be, and are increasingly, monitored for compliance rather than trusted to do the right thing
- smart urban infrastructure reducing the opportunity cost of automatically detecting and penalising minor social infractions (e.g. meter overruns, loud conduct). Perceived benefits must be balanced against the potential effects as a new and potentially coercive stressor on individuals. Any impacts are likely to be disproportionately experienced by marginalised communities already recognised at risk from, for example algorithmic biases (Challen et al., 2019).

Cultural and/or commercial developments that normalise the sharing of detailed personal behavioural information will tend to amplify these consequences. Conversely, strong and user-accessible privacy protections will tend to diffuse them.

E.2 Potential flow-on effects for specific cohorts

A number of impacts and harms linked to the use of IoT for specific cohorts have been articulated in current research. The IoT is likely to exacerbate existing inequalities already faced by vulnerable populations, such as digital literacy or access.

E.2.1 Exacerbating existing inequalities for vulnerable populations

Those with disabilities, the ill, the elderly and those at a socioeconomic disadvantage are at risk through the IoT. Making the provision of crucial services contingent on access to the IoT may aggravate difficulties already faced by vulnerable individuals. The increased dependency of those with disabilities on health, communication or mobility IoT technologies may also make them more ready to accept adverse terms, such as overreaching data collection, use and processing terms or overcharging. These individuals may also be more susceptible to digital consumer manipulation.

There is the possibility that IoT devices might impede access and services to minorities, based on residence, race, ethnicity or socioeconomic status. For example, research published by the Office of the eSafety Commissioner indicates that ethnicity is one factor cited by people experiencing abuse as a reason for being targeted online (Australian eSafety Commissioner, 2020). Flawed data sets and algorithms used in facial recognition technologies have already been blamed for their inability to properly recognise people of colour, and particularly women. Where facial recognition software is used for personal identification, it could present challenges for certain ethnic and social groups to access IoT devices, systems and services. This can lead to problems such as additional screening at airports (Buolamwini and Gebru, 2018).

E.2.2 Gender-related accessibility

Research into the use of energy-related IoT and smart home devices in Australian households (Strengers, 2013; Strengers et al., 2019) found that individuals that instigated and installed these devices were more familiar with these technologies and more likely to be male. In a more comprehensive study from Sweden around energy-saving devices, this disparity is uncovered and the gendered patterns of decision making, subscription and asset custody are mapped (Winther et al., 2019). This disparity necessitates that manufacturers predominantly gear their marketing strategies toward the primary decision-makers, skewing the public perception of the importance and relevance of IoT devices and potentially widening the digital literacy gap.

Women still carry out most domestic activities that consume energy in homes and are more likely to be interested in other ways of enacting environmental responsibility (Farbotko, 2018). Strategies to engage consumers in IoT-enabled energy futures need to take these gendered considerations into account.

There are considerable and unique risks posed to girls and women as part of the current gender divide in digital skills. These were recently detailed in a major global report published by the United National Education, Scientific and Cultural Organisation (UNESCO) EQUALS Skills Coalition (West et al., 2019). The gender skills gap widens for females where technologies are emerging or new, as is the case with the IoT.

E.2.3 Domestic violence

The extent to which the IoT is enabling new forms of domestic violence or other criminal activity is only just beginning to be understood (Bowles, 2018). An emerging body of research is demonstrating worrying trends towards the use of the IoT and smart home devices in exacerbating domestic violence in the home (Bowles, 2018; Leitão, 2018; Strengers et al., 2019). This includes locking occupants in and out of homes or monitoring their movements and engaging in cyber-stalking. Internet-connected thermostats, locks and lights have all been used to enable or otherwise facilitate acts of violence (Bowles, 2018).

The impact of the IoT on questions of liability, and its treatment under the law, is complex and difficult to predict. While new criminal actions could be proposed to deal with this emerging threat, this may not be required. Existing criminal act classifications, including (but not limited to) stalking, fraud, illegal surveillance and possession of a surveillance device may already capture most instances of IoT devices being used for criminal purposes (Domestic Violence Resource Centre Victoria, 2019).

E.2.4 Protecting children from IoT-related harms

The security and privacy concerns associated with the IoT are magnified where IoT devices are used by children. Internet-connected toys directly targeted at children are available (Maras, 2018), and children have indirect access to other IoT devices, such as smart speakers, in the household. Breaches of children's privacy through the IoT have already occurred. An IoT teddy bear was found to have leaked over two million private audio recordings of parents and children due to misconfigured security settings (Goodin, 2017). One analysis of the Amazon 'Echo Dot' smart speaker found that, of the features targeted explicitly at children, more than 80 percent were not covered by a privacy policy (Echo Kids Privacy, 2019).

The Norwegian Customer Council has published research showing that the Bluetooth connection for Genesis Toys' 'My Friend Cayla' and 'i-Que Robot' dolls was completely insecure (no authentication mechanism) and some queries were using insecure HyperText Transfer Protocol (HTTP) connections (subject to a 'man-in-the-middle' attack). The Norwegian Customer Council also found that these dolls recorded anything said to them by children and sent the recordings to US-based Nuance Communications, a specialist in speech recognition. The company reserved the right to share and use the data for a broad range of purposes. Additionally, the Norwegian Customer Council found that the toys were programmed with standard phrases endorsing commercial products, such as Disney movies (ForbrukerRadet (Norwegian Consumer Council), 2016). The study found that 'even the most diligent parent' would not be able to ascertain what information the IoT device was collecting about their children (ForbrukerRadet (Norwegian Consumer Council), 2016)

Australia established the world's first Children's eSafety Commissioner in 2015, whose remit was extended to include all Australians in 2017. In 2019, the Australian Government committed to requiring stronger privacy settings for devices and services marketed to children (Department of Communications and the Arts, 2019). An Online Safety Charter has also been released, and if necessary, the Australian Government will legislate to codify requirements for online service providers to protect users from harmful online experiences (Department of Communications and the Arts, 2019).

E.2.5 Access and inclusion in remote, regional and rural communities

While exclusion from the IoT is different to exclusion from internet access and other connectivity generally, the access and usage of IoT technologies is a barometer for digital inclusion and access in communities. Like most emerging technologies, the IoT is spreading in an inconsistent manner. The 2019 Australian Digital Inclusion Index states that there are significant differences in the digital inclusion score between rural and urban areas, with the score for capital city residents 8.1 points higher for those in rural areas. However the rollout of the NBN has made a discernible impact on narrowing the access gap (Thomas et al., 2019). In RRR communities, personal tracking and health devices for telehealth applications and access to connected mobility services and infrastructure maintenance available through the IoT may be limited by poor connectivity, exacerbating location-based inequalities. It is important for the Australian Government to continue to assess the specific needs and requirements of RRR communities, building on existing work such as the Mobile Black Spot Program and the Regional Connectivity Program, particularly as essential services such as government services, health and education move increasingly to a digital-first model (Australian Government, 2018).

E.2.6 Opting out

The emphasis on IoT inclusion does not provide for individuals or communities who may wish to opt out of the IoT. Potential 'opt out' strategies include choosing not to purchase smart devices, refusing or revoking permissions for data to be shared, and using strategies to anonymise identity in public spaces.

Privacy and surveillance concerns and techno-reactionary viewpoints are also anticipated to result in a substantial minority of individuals choosing to opt out of IoT-enabled services. Those opting-out who are part of the economic elite will be able to use commercial or political influence to circumvent these limitations. As a result, effects will be disproportionately felt by those in already marginalised and disenfranchised communities, potentially compounding negative personal and social consequences.

IoT devices may also lead to a scarcity problem; ordinary, non-IoT versions of customer products may become unavailable. Customers wanting to limit their connectivity to the IoT may find it practically impossible to opt out.

Technical and legal landscapes will substantially shape the extent to which these strategies are feasible or successful (cf. rights under General Data Protection Regulation in Europe versus other regimes).

Governments and policy-makers could consider these issues in urban planning and design. Any reconfiguration of public and/or commercial services regarding smart infrastructure could render customers who wish to opt out unable to access services because they do not have the requisite digital identity or behavioural footprint.

E.2.7 Digital marketing practices

Customers have always been subject to persuasive advertising tactics, but data collected by IoT devices will arguably provide significant advantages to marketers in accuracy, scope, scale and effectiveness. The impact of scale may be amplified by the implementation of software that allows tracking across different customer devices, particularly if done without the knowledge of the customer. At what point do digital marketing practices, particularly those based on sophisticated forms of persuasion, turn the normally 'average' customer into a vulnerable one?[46]

Recent examples include:

- evidence presented to a US enquiry in 2015 asserted that existing smartphone sensors could be used to infer a user's:
  - mood
  - stress levels
  - personality type
  - bipolar disorder
  - demographics (gender, marital status, job status, age)
  - smoking habits
  - overall well-being
  - progression of Parkinson's disease
  - sleep patterns
  - happiness
  - levels of exercise
  - types of physical activity or movement (Manwaring, 2017a)

[46] A recent analysis has concluded that Australia's consumer protection laws are inadequate to protect against this practice, due to the existence of legal problems of *uncertainty* and the failure to protect against a *new harm* (that of corporate secrecy). See L. Goode, 2018.

- in 2017, access to databases containing contact details of 'wheelchair and insulin users, of people addicted to alcohol, drugs, and gambling, as well as suffering from breast cancer, HIV, clinical depression, impotence, and vaginal infections' were offered on a commercial basis (Christi, 2017).

An IoT device with significant autonomy may make decisions that cannot be (or not easily) overridden or that are not obvious to the user due to opacity of the device or the decision-making process. This information can be very valuable to a marketer attempting to persuade customers to buy their products.

Firms may also gain an enhanced ability to engage in forms of 'digital consumer manipulation', targeting customer preferences and exploiting their cognitive biases and individual vulnerabilities.

E.3 Other human rights considerations

In July 2018, the Australian Human Rights Commission released an issues paper as part of its Human Rights and Technology Project, which mentioned briefly that IoT devices could 'present … platforms for cybercrime' (Australian Human Rights Commission, 2018a). However, the challenges raised by IoT devices in relation to human rights extend well beyond cybercrime. As this paper shows, the introduction of IoT devices may have negative implications for human rights regarding privacy, safety, security, non-discrimination and equal treatment (Yu et al., 2018), as well as civil political rights such as freedom of information, opinion and expression, freedom of assembly, and the right to take part in public affairs. The section above discusses challenges for citizens and consumers in relation to privacy and security.

The 2019 protests in Hong Kong provide a potent illustration of perceived problems with IoT devices in relation to civil and political rights to freedom of expression and opinion, freedom of assembly and the right to take part in public affairs. Protesters are shunning the use of smart cards for public transport, for fear of being tracked by law enforcement. Fear of facial recognition technology embedded in IoT devices has led protesters to wear masks and tear down 'smart' lamp posts. The government has denied that such technology is being used in the lamp posts, but the limited visibility of exactly what technology is being used in these particular IoT devices has led to significant distrust (Borak, 2019).

E.4 Perceived community concerns regarding 5G

Electromagnetic fields and radio waves are widely researched areas, with approximately 30,000 studies and reviews worldwide (Australian Radiation Protection and Nuclear Safety Agency, 2019). However, the roll-out of 5G and associated infrastructure has attracted some community interest, particularly around the health impacts from radio waves emitted from mobile telecommunications. Academics and industry generally acknowledge the capabilities of 5G to support many IoT applications over the coming decade, so it is important to consider community concerns about 5G alongside community engagement and education on IoT to increase public trust and acceptance.

E.4.1 Radiofrequency electromagnetic energy

Mobile phone networks (3G and 4G) and other wireless telecommunications sources emit low-level RF EME. This is the transfer of energy by radio waves in the frequency range between 100 and 300 GHz. It is mainly used for telecommunications purposes, including radio and television broadcasting, mobile telephones, WiFi and satellite communications. 5G will initially operate at frequencies similar to 3G and 4G networks. In the future, 5G may begin to operate at higher frequencies, known as millimetre waves (see Figure 19) (Australian Radiation Protection and Nuclear Safety Agency, 2019). However, 5G millimetre waves are still within the spectrum of non-ionising radiation. These will not penetrate the skin and no appreciable heating will occur in the skin (Australian Radiation Protection and Nuclear Safety Agency, 2002).

E.4.2 Current research on RF EME

While exposure to very high levels of RF EME can heat biological tissue and potentially cause tissue damage, the levels of RF EME normally encountered in the environment by the general public are too low to produce harmful effects on human health such as increased body temperature or heating that is deemed significant. This is supported by measurement surveys that have shown that exposure to RF EME in the environment from various sources is very low and typically much lower than the allowable limit for safety in the Australian radiofrequency standard (Karipidis et al., 2017).

While there have been studies reporting a range of biological effects at both high and low levels of RF EME, the results from these studies are sometimes contradictory, providing evidence of no effect (positive or negative) or are inconclusive (Samaras et al., 2015). Overall, these studies do not indicate that exposure constitutes a hazard to human health. Some population health studies have suggested that there could be an association between heavy mobile and cordless phone use and brain cancer (specifically acoustic neuromas); however, limitations of these studies prevent conclusions of causality being drawn from these observations (IARC, 2013). In addition, no long-term effects from RF EME have been proven. There is no established

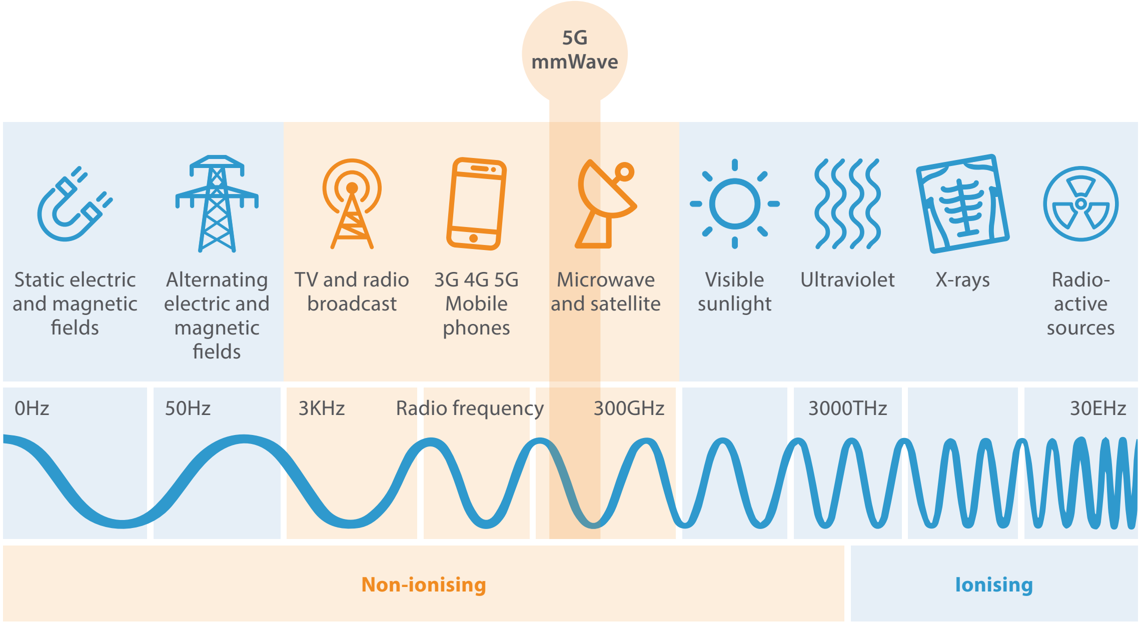


Figure 19: The electromagnetic spectrum

Adapted from ITU, 2020.

scientific evidence that frequencies below this limit, called non-ionising radiation, cause adverse health effects. This is the position of health authorities including ARPANSA, the World Health Organisation (WHO) and International Commission on Non-Ionising Radiation Protection (ICNIRP).

E.4.3 Australian developments on RF EME safety

ARPANSA is responsible for Australia's *Radiation Protection Standard for Maximum Exposure Levels to Radiofrequency Fields*, which sets limits for exposure to RF EME. Compliance with this standard is regulated by the ACMA (Australian Radiation Protection and Nuclear Safety Agency, 2002). These limits are set well below levels at which harm to people may occur.

Millimetre wave frequencies are covered by ARPANSA's current standard (Australian Radiation Protection and Nuclear Safety Agency, 2019). The operating frequencies of the 5G network (as well as current 3G and 4G networks) are within this limit set by the ARPANSA Standard. ARPANSA's overall assessment is that 5G is safe (Australian Radiation Protection and Nuclear Safety Agency, 2019).

In late 2019, the Australian Government announced a $9 million package over four years for more research into electromagnetic energy from telecommunications facilities to build public confidence in the safety of telecommunications networks, including 5G mobile networks. With this funding, ARPANSA will deliver targeted research and measurement studies. Outcomes of this research will be included in clear and more accessible information for the public about electromagnetic energy from telecommunications facilities (Minister for Health, 2020).

In March 2020, the ICNIRP released its updated guidelines for limiting exposure to electromagnetic fields, which provide authoritative advice on radiation protection, which are relied on by the WHO. The updated guidelines provide explanations of how exposure limits have been set, as well as a review of current research into radio waves and health. This covers many applications including 5G technologies, WiFi, Bluetooth, mobile phones and base stations (International Commission on Non-Ionizing Radiation Protection (ICNIRP), 2020). ARPANSA's standard will be updated during 2020 to ensure alignment with the new updated guidelines (Australian Radiation Protection and Nuclear Safety Agency, 2020).

Although the body of science demonstrates that there are no health effects from radio waves in mobile telecommunications, it is important to continue the research in radiation safety. ARPANSA has provided recommendations for areas of research to expand existing knowledge, including the ongoing assessment of personal and environmental exposure to radio waves from new and emerging technologies such as the use of millimetre wave spectrum (Australian Radiation Protection and Nuclear Safety Agency, 2017). Over the next decade, it will be important to continue the research and to consider community education, in order to reassure the Australian population about any perceived health impacts of telecommunications technologies, including 5G.

APPENDIX F
INTERNATIONAL USE CASES

F.1 Retail

Automated grocery logistics warehouse – Ocado

Ocado, a British online-only supermarket, has developed a highly automated 'grid' structure warehouse using an IoT smart platform and robots to fulfil grocery orders. Robots perform simple tasks (like lifting, moving and sorting), using their central cavity and a set of claws to grab crates of items and move them to a new location, or drop them down a vertical chute to a picking station. At these stations, human employees take the items and place them in shopping bags in different crates. Crates are then sent back into the grid to be refilled with items or, once filled, moved onto a delivery bay to be sent to customers.

The Ocado Smart Platform is an end-to-end e-commerce solution for operating online retail businesses. It combines their end-to-end software and technology systems using a cloud-based architecture that allows the platform to be scalable and continuously updated.

Evaluation: Ocado is selling its propriety software and hardware platform to other retail partners including Morrisons, ICA and Coles. Their Smart Platform is fully scalable and can be configured to suit each retailer's specific needs. Their automated fulfilment platform is also scalable and can fit into existing warehouses, using space more efficiently. Ocado's system of an integrated end-to-end platform is unique and is likely to be applicable across e-commerce and advanced manufacturing sectors.

Smart shelves – Giant Eagle

US-based grocery chain Giant Eagle deploys smart shelves in their stores. Sensors and dashboards measure inventory life and send shoppers product information on their mobile phones. Giant Eagle has reduced its out-of-stock replenishment time by two-thirds and cut its out-of-stock items by 50 percent on any given day.

Evaluation: Smart shelves are a high-potential use case according to Capgemini, due to fast return on investment and overall benefit from implementation.

F.2 Infrastructure

Using IoT technology in predictive modelling and building of infrastructure to reduce waste – ARUP

Arup, a British design and construction firm, has been exploring IoT-solutions to facilitate predictive maintenance to enable circularity of buildings and infrastructure constructions. They have developed a full integrated structural health monitoring system, which comprises 1,000 sensors to provide continuous, real-time data on the condition of buildings and infrastructure. The sensor system provides advance warnings of structural problems and allows for predictive maintenance. This system was used to provide data on a newly constructed bridge across the River Forth, to ensure the smooth operation of the bridge and to prolong its service life.

Evaluation: Arup demonstrates how the IoT can be used to monitor construction projects and enable predictive maintenance in a sector where the longevity of assets has traditionally been an obstacle. By using the IoT and data to track ownership and condition of assets, suppliers are able to retain the asset while optimising performance. For example, steel manufacturers could provide 'steel as a service'. The asset could be reused in different projects, thereby reducing waste. Similarly, if buildings are intelligently designed out waste (with the condition and ownership structure of all its components made transparent), then maintenance, repairs and services could be looped to accommodate changing needs or technology upgrades.

F.3 Advanced manufacturing

Asset tracking and production asset maintenance – Rolls-Royce Holdings

Rolls-Royce, one of the world's largest jet engine manufacturers, uses the IoT to increase fuel efficiency of jet engines, optimise flight paths and for predictive maintenance. Sensors fitted inside aircraft engines track engine health, air traffic control, route restrictions and fuel use to diagnose potential faults or operational anomalies. This system provides real-time information on engine performance mid-flight, allowing Rolls-Royce to carry out predictive maintenance. This reduces not only the frequency of unexpected or severe faults, but also improves engine efficiency and lowers fuel consumption. Rolls-Royce Holdings estimates that a one percent reduction in fuel usage equates to savings of US$250,000 per plane per year.

Evaluation: This example demonstrates how the IoT can be deployed by businesses to track and monitor physical assets to optimise performance and extend their lifecycle. This use case has applicability across sectors that use physical assets, including advanced manufacturing, utilities management, logistics and retail.

F.4 Utility management

Pay-as-you-go solar energy – Angaza

Angaza's pay-as-you-go platform facilitates the sale of solar-powered devices to people in emerging markets throughout Africa, South America and Southeast Asia. Their business model is a combination of usage monitoring system and micro-financing, and its pay-as-you-go platform supports manufacturers who want to sell their products in emerging markets. The products are embedded with sensors that monitor energy use. Customers are able to buy products for a small down payment. Once in use, the sensors monitor energy use or time used, and automatically deactivate products if the pre-paid usage/time is expended and another payment is not made by the customer. After the payments have exceeded a defined retail price, a customer can use the product free of any further charge.

Evaluation: Knowledge of the condition of the asset allows Angaza's customers (i.e. manufacturers) to charge users for the usage of the product rather than for the product itself. For example, a user can obtain an inexpensive solar-powered reading light, paying on a weekly basis with unlimited use or per kWh of usage, rather than paying the traditional retail price for the product. In underdeveloped areas, access to a lamp can mean the difference between achieving a university degree or remaining in poverty. This model also increases the utility of the asset, where acquired data in products with a Global System for Mobile communications chip can be leveraged for predictive maintenance of products. A more profound, indirect consequence of this model is the potential to support developing and remote regions to transition to a grid-free, renewable powered society, without the massive infrastructure investments that would be required to develop a conventional grid.

Angaza's model demonstrates how traditional retail business models could potentially be transformed into pay-as-you-go service models. This has an important role in creating a circular economy, where data from IoT-enabled products could be used in predictive maintenance and recall of materials in products for reusing and recycling. Aggregate data could also be used in product design to create more sustainable and efficient products.

Decentralised solar-energy grid – Okra Solar

Okra Solar has developed an IoT solar home system designed to enable poorer communities to live off the grid, by establishing microgrids that can be used to distribute power to households. Excess energy can also be distributed through the network to neighbouring households that require extra power. They work with their partners in these communities to install their solar panel hardware, which connects to Okra's smart software system to create a decentralised energy grid. Mobile payments, autonomous power distribution, maintenance and scaling, network updates and upgrades are all managed online through their system, with monitoring and reports on grid activity being sent to the cloud in real time. Their modular architecture also allows any household to connect to a pre-existing Okra grid from two households upwards to form clusters.

Evaluation: Okra's decentralised grid system is an example of how IoT technology can be used to provide low-cost solutions to deliver energy to lower socioeconomic communities. Community engagement and ownership of energy production and supply is also likely to improve digital literacy, enhance understanding of energy use and supply, and encourage local entrepreneurship.

F.5 Transport

Truck platooning

Truck platooning involves a number of trucks closely following one another, connected using V2V communication. While not currently in use, the system could be based on adaptive cruise control (comprising on-board radar and other electronic equipment), with each truck optimising its behaviour using V2V communication. The aim is to enable fuel savings and reductions in carbon dioxide emissions through trucks following each other closely. A number of companies are actively engaged in developing this technology, including Peloton Technology, Scania, Daimler, Hino and others. In order to use public road networks, further testing and supporting legislative change will be required. It is not anticipated that automated driverless truck platooning will be commercially available until at least 2030.

Evaluation: Truck platooning demonstrates how IoT technology can be used to increase efficiencies, reduce fuel consumption and provide aggregated data to optimise a company's business model. However, there are a wide range of social impacts that need to be considered, from greater employee satisfaction from reduced hours on the road, to issues concerning job security and automation. Safety and regulation will also be key issues before this technology can be deployed.

On-demand air taxi services – Lilium/Uber/Rolls-Royce Holdings

A number of companies including Lilium and Uber are trialling air vehicles to provide on-demand air taxi services.

Evaluation: On-demand air taxi services have the potential to revolutionise urban travel and cut down on travelling times across congested cities or regions. However, challenges include gaining public acceptance, building the necessary infrastructure to support the take-off/landing of these vehicles, as well as meeting the regulatory demands of navigating the air space above cities and regions. These services will also need to be cost-competitive and avoid interference with commercial planes and smaller aircraft industries.

F.6 Sustainability

Disease control – International Cooperation for Animal Research using Space

Researchers are exploring ways of integrating the IoT and nature to increase our understanding of the natural world. Teams from the International Cooperation for Animal Research using Space (the German–Russian observation system for animal movements) are seeking to understand animal migration. They are equipping species such as bats and geese with miniature transmitters that send their measurement data to the International Space Station and then back to a ground station.

The Centres for Disease Control and Prevention estimates that more than six out of 10 infectious diseases are passed between animals and humans. In one project, Swedish mallard ducks were implanted with sensors to record not only location, but also body temperature to monitor the spread of avian influenza. Temperature readouts could identify infected individuals. Coupled with geographic data of migration routes, researchers could track where birds contract and transmit disease. This model has the potential to improve the accuracy of disease outbreak prediction and planning interventions before an epidemic occurs.

Internet of Bees – University of Washington

The University of Washington has developed a biology-based solution to integrate sensing, computing and communication functionalities onto live, flying insects to create a mobile IoT platform. Sensors, data storage, receivers for location tracking and a rechargeable battery were able to be loaded into a 102-milligram package that can be attached onto bumblebees. As the bees go about their everyday activity, sensors measure temperature and humidity, and their position can be tracked via radio signal. Once they return to the hive, the data are uploaded and the battery recharges wirelessly.

Evaluation: These trials demonstrate how IoT sensors can leverage biology to provide new environmental monitoring opportunities. Aside from being able to provide data for agricultural purposes to monitor pests, weather conditions or crop health, these sensors could also be used to monitor the impacts of climate change, as well as the effects of deforestation on endangered species.

F.7 Disaster management

Fire warning and alert system – Red Cross

In Nairobi and Cape Town, the Red Cross is piloting a system of connected alarms across high density urban slums to notify residents of fast-moving fires. The use of low-cost solar powered sensors networked together to quickly detect and relay information to authorities is currently being explored. The network sounds alarms, communicates to threatened residents (via SMS and other modalities) and connected sensors identify the origin of the fire via GPS, notifying authorities of the location where fire mitigation efforts should be targeted (Biggs et al., 2016).

Evaluation: This example could be used to support fire response and management in RRR areas in Australia, minimising cost and utilising solar energy.

GLOSSARY

Application program interface	A set of specifications that enables intermediary software to facilitate the communication between two systems.
Automated vehicle	Vehicles where the tasks associated with driving, including accelerating, braking, turning or changing lanes will be performed by an automated intelligent system rather than a human driver.
Augmented reality	Technology that superimposes a computer-generated image on a user's view of the real world, thus providing a composite view.
CAT-M1	A low-power wide area network that functions on a 1.4 MHz spectrum and provides average upload speeds between 200 Kbps and 400 Kbps. It provides wide area coverage and has low power requirements but has smaller data bandwidth capabilities.
Cyber-physical systems	Technologies that bring the virtual and material dimensions together to produce a fully networked domain, in which intelligent objects interact with each other.
Data wrangling	Process of cleaning and unifying complex 'raw' data sets into a desired useable format.
Digital twin	A digital twin is a digital representation of a physical object or system, which uses technology to capture real-time data for process analytics and predictive maintenance of machines. Digital twins are physics-based and focused on the product, process and performance of the product and process. This technology goes beyond current visualisation and conventional engineering simulation tools by integrating these in the twin.
Edge computing	Computing and storage systems that process data at 'the edge', as close as possible to the component, device, application or human that produces the data being processed, rather than sending data to a central processing system. The purpose is to reduce latency, as data does not need to be sent to the central processing system and then back to the edge.
Field-programmable gate array	A field-programmable gate array is an integrated circuit that can be reprogrammed or configured by a customer or designer after manufacturing. This can be used to perform a specific task with high performance and reliability. The flexibility and scalability of these arrays makes them useful for many applications in the IoT, such as enabling high-performance and real-time video analytics for infrastructure management in smart cities or to manage data aggregation in healthcare systems.
Fog computing	Architecture required to bring cloud computing capabilities to the edge of the network. This enables enterprises to push computing processing out of centralised systems or clouds for more efficient and scalable performance.
Government as a Platform	Government as a Platform represents a model for digital transformation of public services.

General-purpose graphics processing unit

A general-purpose graphics processing unit is a graphics processing unit that is used for purposes other than rendering graphics. Multicore parallel processing abilities enable increased speed and capability to perform operations quickly, making it useful for big data analytics.

Global System for Mobile Communications (GSM)

A standard developed by the European Telecommunications Standards Institute for second-generation (2G) digital cellular networks used by mobile devices.

Internet of Things

An ecosystem in which applications and services are driven by data collected from devices that sense and interface with the physical world. In the Internet of Things, devices and objects have communication connectivity, either a direct connection to the internet or mediated through local or wide area networks.

IoT devices

Objects (including buildings and living things) that are not inherently computerised, but into which have been embedded one or more computer processors with data collection, data handling and data communication capabilities. IoT devices may have interactions with living things, the physical world, other IoT devices and other computing devices or systems.

Industry 4.0

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

Latency

Time it takes for a data packet to travel from its origin point to its destination. The type of connectivity and distance also impact on latency.

Narrowband-IoT

A low power wide area network radio technology standard developed by the 3rd Generation Partnership Project that meets requirements for extended coverage and low-device complexity.

Pervasive computing

Entails building models of the environment in which technology is embedded in the context of use.

Platform urbanism

Using advances in the IoT and data analytics to extend the reach of platform ecosystems into urban domains.

Ubiquitous computing

Addition of mobility to computing, so the environment and its context of use can entirely change, requiring dynamic configuration.

Vendor lock-in

Customers are dependent on a single technology provider’s implementation, which may restrict future ability to move to a different vendor without substantial costs, legal constraints or technological incompatibilities.

ABBREVIATIONS

ACMA	Australian Communications and Media Authority
ACCC	Australian Competition and Consumer Commission
ACOLA	Australian Council of Learned Academies
AI	artificial intelligence
API	application program interface
APP	Australian Privacy Principles
AR	augmented reality
ARC	Australian Research Council
ARPANSA	Australian Radiation Protection and Nuclear Safety Agency
CAVs	connected and automated vehicles
CO	carbon monoxide
CO2	carbon dioxide
COVID-19	coronavirus disease
CRC	Cooperative Research Centre
CSIRO	Commonwealth Scientific and Industrial Research Organisation
DSA	dynamic spectrum access
EHR	Electronic Health Record
EMR	Electronic Medical Record
EU	European Union
ETSI	European Telecommunications Standards Institute
FTTH	Fibre to the Home
FTTP	Fibre to the Premise
GaaP	government as a platform
GDP	gross domestic product
GLAM	galleries, libraries, archives and museums
GPS	Global positioning system
GSM	Global Standard for Mobile Communications
HAPS	high-altitude pseudo satellites
ICT	information and communications technology
IEEE	Institute of Electrical and Electronics Engineers
IIoT	industrial Internet of Things
IoT	Internet of Things
IoTAA	Internet of Things Alliance Australia

IP	Internet Protocol
ISO	International Organization for Standardization
ITS Australia	Intelligent Transport Systems Australia
ITU	International Telecommunication Union
LEO	low-earth orbit
LGA	Local government area
LoRa	long range
LoRaWAN	long range wide area network
LPWAN	low power wide area network
LTE	long-term evolution
LTE-M	long-term evolution machine-type communication
M2M	machine-to-machine
MaaS	mobility as a service
NB-IoT	narrowband-Internet of Things
NBN	national broadband network
NSW	New South Wales
OAIC	Office of the Australian Information Commissioner
OECD	Organisation for Economic Co-operation and Development
ONDC	Office of the National Data Commissioner
PHR	Personal Health Record
PwC	PricewaterhouseCoopers
R&D	research and development
RF EME	radiofrequency electromagnetic energy
RRR	rural, regional and remote
SME	small to medium enterprises
UK	United Kingdom
URLLC	ultra-reliable low-latency communication
US	United States
V2X	vehicular communication
VET	vocational education and training
VR	virtual reality
WA	Western Australia
WHO	World Health Organization

REFERENCES

Abbasi, M., Vassilopoulou, P., and Stergioulas, L. (2017). Technology roadmap for the Creative Industries. *Creative Industries Journal*, *10*(1), 40–58. https://doi.org/10.1080/17510694.2016.1247627

Abduljabbar, R., Dia, H., Liyanage, S., and Bagolee, S. A. (2019). Applications of Artificial Intelligence in Transport: An Overview. *Sustainability*, *11*(1), 189. https://doi.org/https://doi.org/10.3390/su11010189

Adams, J. (2019). *Darwin Promises Not to Deploy Live Face Recognition in $A10 Million Smart City Solution*. Security Electronics and Networks. https://securityelectronicsandnetworks.com/articles/2019/08/20/darwin-promises-not-to-deploy-live-face-recognition-in-a10-million-smart-city-solution/

Adegbija, T., Rogacs, A., Patel, C., and Gordon-Ross, A. (2018). Microprocessor Optimizations for the Internet of Things: A Survey. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, *37*(1), 7–20. https://doi.org/10.1109/TCAD.2017.2717782

Adila, A. S., Husam, A., and Husi, G. (2018). Towards the self-powered Internet of Things (IoT) by energy harvesting: Trends and technologies for green IoT. *2018 2nd International Symposium on Small-Scale Intelligent Manufacturing Systems (SIMS)*, 1–5. https://doi.org/10.1109/SIMS.2018.8355305

Ahlgren, B., Dannewitz, C., Imbrenda, C., Kutscher, D., and Ohlman, B. (2012). A Survey of Information-Centric Networking. *IEEE Communications Magazine*, *50*(7), 26–36. https://doi.org/10.1109/MCOM.2012.6231276

AiGroup. (2018). *Industry 4.0 Higher Apprenticeships Program*. https://cdn.aigroup.com.au/Reports/2018/Industry_4_Higher_Apprenticeship_Program_July_2018.pdf

AlphaBeta. (2017). *The Automation Advantage: How Australia can seize a $2 trillion opportunity from automation and create millions of safer, more meaningful and more valuable jobs.* https://www.alphabeta.com/wp-content/uploads/2017/08/The-Automation-Advantage.pdf

Anaissi, A., Nguyen, K., Rakotoarivelo, T., Makki Alamdari, M., and Wang, Y. (2019). Smart pothole detection system using vehicle-mounted sensors and machine learning. *Journal of Civil Structural Health Monitoring*, *9*, 91–102. https://doi.org/10.1007/s13349-019-00323-0

Anastasiu, I., Foth, M., Schroeter, R., and Rittenbruch, M. (2020). From Repositories to Switchboards: Local Governments as Open Data Facilitators. In S. Hawken, H. Han, & C. Pettit (Eds.), *Open Cities|Open Data* (pp. 331–358). Palgrave Macmillan, Singapore. https://doi.org/10.1007/978-981-13-6605-5_15

Andrae, A., and Corcoran, P. M. (2013). *Emerging trends in electricity consumption for consumer ICT*.

Ang, L.-M., Seng, K. P., Ijemaru, G. K., and Adamu, M. Z. (2018). Deployment of IoV for Smart Cities: Applications, Architecture and Challenges. *IEEE Access*, *7*, 6473–6492. https://doi.org/10.1109/ACCESS.2018.2887076

Arrobas, D. L. P., Hund, K. L., Mccormick, M. S., Ningthoujam, J., and Drexhage, J. R. (2017). *The Growing Role of Minerals and Metals for a Low Carbon Future*. http://documents.worldbank.org/curated/en/207371500386458722/pdf/117581-WP-P159838-PUBLIC-ClimateSmartMiningJuly.pdf

Arup, University College London, and Smart City Expo. (2014). *Delivering the Smart City: Governing Cities in the Digital Age*. https://www.arup.com/perspectives/publications/research/section/delivering-the-smart-city

Ashton, K. (2019). Darwin council promises not to use facial recognition technology in new CCTV cameras. *ABC News*. https://www.abc.net.au/news/2019-08-19/darwin-cctv-facial-recognition-technology-raises-concerns/11425822

Assante, D., Romano, E., Flamini, M., Castro, M., Martín, S., Lavirotte, S., Rey, G., Leisenberg, M., Migliori, M., Bagdoniene, I., Gallo, R. T., Pascoal, A., and Spatafora, M. (2018). Internet of Things education: Labor market training needs and national policies. *2018 IEEE Global Engineering Education Conference (EDUCON)*, 1846–1853. https://doi.org/10.1109/EDUCON.2018.8363459

Australian Bureau of Statistics. (2018). *8146.0 - Household Use of Information Technology, 2016-7*. https://www.abs.gov.au/ausstats/abs@.nsf/mf/8146.0

Australian Bureau of Statistics. (2019). *9309.0 - Motor Vehicle Census, Australia, 31 Jan 2019*. https://www.abs.gov.au/ausstats/abs@.nsf/mf/9309.0

Australian Communications and Media Authority. (2015). *The Internet of Things and the ACMA's areas of focus: Emerging issues in media and communications Occasional Paper*. https://www.acma.gov.au/publications/2015-11/report/internet-things-and-acmas-area-focus-emerging-issues-occasional-paper

Australian Communications and Media Authority. (2019a). *Communications Report 17-18*. https://www.acma.gov.au/sites/default/files/2019-08/Communications report 2017-18.pdf

Australian Communications and Media Authority. (2019b). *Five-year spectrum outlook 2019-23: The ACMA's spectrum work program*. https://www.acma.gov.au/sites/default/files/2019-08/Internet of Things_occasional paper pdf.pdf

Australian Communications and Media Authority. (2019c). *New approaches to spectrum sharing - consultation 25/2019*. https://www.acma.gov.au/consultations/2019-10/new-approaches-spectrum-sharing-consultation-252019

Australian Communications and Media Authority. (2020a). *Communications Report 2018-19*. https://www.acma.gov.au/sites/default/files/2020-02/Communications report 2018-19.pdf

Australian Communications and Media Authority. (2020b). *Impacts of the 2019-20 bushfires on the telecommunications network*. https://www.acma.gov.au/publications/2020-04/report/impacts-2019-20-bushfires-telecommunications-network

Australian Competition and Consumer Commission. (2019a). *Digital Platforms Inquiry Final Report*. https://www.accc.gov.au/system/files/Digital platforms inquiry - final report.pdf

Australian Competition and Consumer Commission. (2019b). *Product Safety Priorities 2019*. https://www.accc.gov.au/about-us/australian-competition-consumer-commission/product-safety-priorities-2019

Australian Competition and Consumer Commission. (2020). *Agricultural machinery: after-sales markets*. https://www.accc.gov.au/focus-areas/agriculture/agricultural-machinery-after-sales-markets

Australian Energy Market Operator (AEMO). (2020). *Power of Choice*. https://www.aemo.com.au/initiatives/major-programs/past-major-programs/nem-power-of-choice

Australian eSafety Commissioner. (2019). *Safety by Design Overview*. https://www.esafety.gov.au/sites/default/files/2019-10/SBD - Overview May19.pdf

Australian eSafety Commissioner. (2020). *Online hate speech: findings from Australia, New Zealand and Europe*. https://www.esafety.gov.au/sites/default/files/2020-01/Hate speech-Report.pdf

Australian Government. (2004). *A hand up not a hand out: Renewing the fight against poverty (Report on poverty and financial hardship)*.

Australian Government. (2018). *2018 Regional Telecommunications Review: Getting it right out there*.

Australian Government. (2019a). *Australia's 2020 Cyber Security Strategy A Call for views*. https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-strategy-2020-discussion-paper.pdf

Australian Government. (2019b). *Draft Code of Practice: Securing the Internet of Things for Consumers*. https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf

Australian Government. (2019c). *Strengthening Skills Expert Review of Australia's Vocational Education and Training System*. https://pmc.gov.au/sites/default/files/publications/strengthening-skills-independent-review-australia-vets.pdf

Australian Government, and Australian Space Agency. (2019). *Advancing Space: Australian Civil Space Strategy 2019-2028*. https://publications.industry.gov.au/publications/advancing-space-australian-civil-space-strategy-2019-2028.pdf

Australian Government, and Department of Infrastructure, Regional Development and Cities. (2018). *Smart Cities Plan Launceston City Deal: Annual Progress Report July 2018*. https://www.infrastructure.gov.au/cities/city-deals/launceston/files/launceston-annual-progress-report-2018.pdf

Australian Human Rights Commission. (2018a). *Human Rights and Technology Issues Paper*. https://www.humanrights.gov.au/sites/default/files/document/publication/AHRC-Human-Rights-Tech-IP.pdf

Australian Human Rights Commission. (2018b). *Human Rights and Technology Issues Paper*. https://www.humanrights.gov.au/sites/default/files/document/publication/AHRC-Human-Rights-Tech-IP.pdf

Australian Human Rights Commission. (2019). *Human Rights and Technology: Discussion Paper 2019*.

Australian Institute of Health and Welfare. (2019). *Australian Burden of Disease Study: Impacts and causes of illness and death in Australia*. https://www.aihw.gov.au/getmedia/c076f42f-61ea-4348-9c0a-d996353e838f/aihw-bod-22.pdf.aspx?inline=true

Australian Law Reform Commission. (2008). *For Your Information: Australian Privacy Law and Practice (ALRC Report 108)*. https://www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/

Australian Privacy Foundation. (2018). *Australian State and Territory Privacy Laws*. https://privacy.org.au/resources/privacy-law/plawsst/

Australian Radiation Protection and Nuclear Safety Agency. (2002). *Radiation Protection Standard: Maximum Exposure Levels to Radiofrequency Fields - 3 kHz to 300 GHz*. https://www.arpansa.gov.au/sites/default/files/legacy/pubs/rps/rps3.pdf?acsf_files_redirect

Australian Radiation Protection and Nuclear Safety Agency. (2017). *Radiofrequency Electromagnetic Energy and Health: Research Needs*. https://www.arpansa.gov.au/sites/default/files/tr178.pdf

Australian Radiation Protection and Nuclear Safety Agency. (2019). *Submission to the House of Representations Standing Committee on Communications and the Arts Inquiry into 5G in Australia*. https://www.arpansa.gov.au/sites/default/files/arpansa_submission_to_inquiry_into_5g_in_australia_1.pdf

Australian Radiation Protection and Nuclear Safety Agency. (2020). *Updated international radiation safety guidelines*. https://www.arpansa.gov.au/news/updated-international-radiation-safety-guidelines

Australian Trade and Investment Commission. (2020). *Export markets - Republic of Korea*. https://www.austrade.gov.au/Australian/Export/Export-markets/Countries/Republic-of-Korea/Market-profile

Bain & Company. (2018). *Bain & Company predict the Internet of Things market will more than double to $520 billion by 2021*. https://www.bain.com/about/media-center/press-releases/2018/bain-predicts-the-iot-market-will-more-than-double-by-2021

Baldini, G., Botterman, M., Neisse, R., and Tallacchini, M. (2016). Ethical Design in the Internet of Things. *Science and Engineering Ethics*, *24*. https://doi.org/10.1007/s11948-016-9754-5

Bandyopadhyay, S., Sengupta, M., Maiti, S., and Dutta, S. (2011). Role Of Middleware For Internet Of Things: A Study. *International Journal of Computer Science & Engineering Survey*, *2*(3). https://doi.org/10.5121/ijcses.2011.2307

Barns, S. (2019a). *The Internet of Things (IoT) and key issues for future services*.

Barns, S. (2019b). Negotiating the platform pivot: From participatory digital ecosystems to infrastructures of everyday life. *Geography Compass*. https://doi.org/10.1111/gec3.12464

Barns, S., Cosgrave, E., Acuto, M., and Mcneill, D. (2017). Digital Infrastructures and Urban Governance. *Urban Policy and Research*, *35*(1), 20–31. https://doi.org/10.1080/08111146.2016.1235032

Batty, M. (2013). Big data, smart cities and city planning. *Dialogues in Human Geography*, *3*(3), 274–279. https://doi.org/10.1177/2043820613513390

Bennett Moses, L. (2007). Recurring dilemmas: The law's race to keep up with technological change. *University of Illinois Journal of Law, Technology & Policy*, 239.

Best, K. (2010). Living in the control society: Surveillance, users and digital screen technologies. *International Journal of Cultural Studies*, *13*, 5–24. https://doi.org/10.1177/1367877909348536

Bhatt, Y., and Bhatt, C. (2017). Internet of things in healthcare. In C. Bhatt, N. Dey, & A. S. Ashour (Eds.), *Internet of things and big data technologies for next generation healthcare* (pp. 13–33). Springer.

Bica, I., Chifor, B.-C., Arseni, Ștefan-C., and Matei, I. (2019). Multi-Layer IoT Security Framework for Ambient Intelligence Environments. *Sensors (Basel, Switzerland)*, *19*(18), 4038. https://doi.org/10.3390/s19184038

Biggs, P., Garrity, J., LaSalle, C., and Polomska, A. (2016). *Harnessing the Internet of Things for Global Development*. https://www.itu.int/en/action/broadband/Documents/Harnessing-IoT-Global-Development.pdf

Bleischwitz, R. (2014). *Supplies of rare earth materials are still far from secure*. The Conversation. https://theconversation.com/supplies-of-rare-earth-materials-are-still-far-from-secure-33156

Blythe, J., and Lefevre, C. (2018). *Cyberhygiene Insight Report*. https://iotuk.org.uk/wp-content/uploads/2018/01/PETRAS-IoTUK-Cyberhygiene-Insight-Report.pdf

Bogle, A. (2018, January 30). Strava has published details about secret military bases, and an Australian was the first to know. *ABC News*. https://www.abc.net.au/news/science/2018-01-29/strava-heat-map-shows-military-bases-and-supply- routes/9369490

Borak, M. (2019, August 30). Why are Hong Kong protesters targeting lamp posts? *South China Morning Post*. https://www.scmp.com/tech/big-tech/article/3024997/why-are-hong-kong-protesters-targeting-lamp-posts

Bosua, R., Richardson, M., Clark, K., Maynard, S., Ahmad, A., and Webb, J. (2017). *Privacy in a World of the Internet of Things: A Legal and Regulatory Perspective* (Networked Society Institute Research Paper 6; Networked Society Institute Research Paper 6).

Bowles, N. (2018, June 23). Thermostats, Locks and Lights: Digital Tools of Domestic Abuse. *The New York Times*. nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html

Boxall, N. J., King, S., Kaksonen, A., Bruckard, W., and Roberts, D. (2019). *Waste Innovation for a Circular Economy: A summary report for the CSIRO Cutting Edge Science and Engineering Symposium*. https://publications.csiro.au/rpr/download?pid=csiro:EP195506&dsid=DS4

Boyd, J. (2019, February 20). Japan to Probe IoT Devices and Then Prod Users to Smarten Up. *IEEE Spectrum*. https://spectrum.ieee.org/tech-talk/telecom/internet/japan-aims-to-probe-unsecured-iot-devices-and-then-prod-users-to-smarten-up

Bradford, N., Caffery, L., and Smith, A. (2016). Telehealth services in rural and remote Australia: a systematic review of models of care and factors influencing success and sustainability. *Rural and Remote Health*, *16*(4). https://www.rrh.org.au/journal/article/4268

Bradlow, H. (2019). *The Internet of Things Presentation*.

Brakewood, C., and Watkins, K. (2018). A literature review of the passenger benefits of real-time transit information. *Transport Reviews*, 1–30. https://doi.org/10.1080/01441647.2018.1472147

Brass, I., Pothong, K., Tanczer, L., and Carr, M. (2019). Standards, Governance and Policy. In K. Pothong, I. Brass, & M. (eds) Carr (Eds.), *Cybersecurity of the Internet of Things: PETRAS Stream Report*. Petras IoT Research Hub. https://doi.org/10.13140/RG.2.2.15925.42729

Briner, J. (2019, March 5). Energy Harvesting for IoT Devices. *IoT for All*. https://www.iotforall.com/energy-harvesting-iot-devices/

Brownsword, R. (2008). *Rights, regulation and the technological revolution*. Oxford University Press, Inc.

Brumaghin, E., Gibb, R., Mercer, W., Molyett, M., and Williams, C. (2017). *CCleanup: A Vast Number of Machines at Risk*. https://blog.talosintelligence.com/2017/09/avast-distributes-malware.html

Buhr, D. (2015). *Industry 4.0 – New Tasks for Innovation Policy*. https://library.fes.de/pdf-files/wiso/11480.pdf

Bulkeley, H., Coenen, L., Frantzeskaki, N., Hartmann, C., Kronsell, A., Mai, L., Marvin, S., McCormick, K., Steenbergen, F., and Voytenko Palgan, Y. (2016). Urban living labs: governing urban sustainability transitions. *Current Opinion in Environmental Sustainability*, *22*, 13–17. https://doi.org/10.1016/j.cosust.2017.02.003

Buntz, B. (2019). *5 Cybersecurity Lessons Related to IP Security Cameras*. IoT World Today. https://www.iotworldtoday.com/2019/08/31/5-cybersecurity-lessons-related-to-ip-security-cameras/

Bunz, M., and Meikle, G. (2018). *The Internet of Things*. Polity Press.

Buolamwini, J., and Gebru, T. (2018). *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*. http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

Bureau of Communications and Arts Research. (2020). *Measuring the digitalisation of Australia's economy 2012-13 to 2016-17: Mapping the economic contribution for IoT, ICT and digital activity in Australia*.

Bureau of Infrastructure, Transport and Regional Economics (BITRE). (2015). *Traffic and congestion cost trends for Australian capital cities, Information Sheet 74*. https://www.bitre.gov.au/sites/default/files/is_074.pdf

Burke, S. (2013, September 23). HP haven big data platform is gaining partner momentum. *CRN*, 2013. https://www.crn.com/news/applications-os/240161649/hp-haven-big-data-platform-is-gaining-partner-momentum.htm

Burrows, A., Bradburn, J., and Cohen, T. (2014). *Journeys of the Future: Introducing Mobility as a Service.* https://www.atkinsglobal.com/~/media/Files/A/Atkins-Corporate/uk-and-europe/uk-thought-leadership/reports/Journeys of the future_300315.pdf

Calabresi, G. (1970). *The Costs of Accidents*. Yale University Press.

SB-327 Information privacy: connected devices, (2018) (testimony of Californian Senate). https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327

Caprotti, F., and Cowley, R. (2018). Varieties of smart urbanism in the UK: Discursive logics, the state and local urban context. *Transactions (Institute of British Geographers)*. https://doi.org/10.1111/tran.12284

Cardinia Shire Council. (2019). *Maintaining unsealed roads*. https://www.cardinia.vic.gov.au/info/20006/roads_footpaths_and_drains/736/maintaining_unsealed_roads#section-10-driving-on-unsealed-roads-

Castellazzi, L., Maria, A., and Bertoldi, P. (2017). *Trends in data centre energy consumption under the European Code of Conduct for data centre energy efficiency*. https://doi.org/10.2760/358256

Challen, R., Denny, J., Pitt, M., Gompels, L., Edwards, T., and Tsaneva-Atanasova, K. (2019). Artificial intelligence, bias and clinical safety. *BMJ Quality & Safety*, *28*, 231–237. https://doi.org/10.1136/bmjqs-2018-008370

Chartered Accountants Australia and New Zealand, and Deloitte Access Economics. (2016). The Future of Work: How can we adapt to survive and thrive? In *future[inc]*. https://www.voced.edu.au/content/ngv%3A71996

Chatfield, A. T., and Reddick, C. G. (2019). A framework for Internet of Things-enabled smart government: A case of IoT cybersecurity policies and use cases in U.S. federal government. *Government Information Quarterly*, *36*(2), 346–357. https://doi.org/https://doi.org/10.1016/j.giq.2018.09.007

Chiang, M., and Zhang, T. (2016). Fog and IoT: An Overview of Research Opportunities. *IEEE Internet of Things Journal*, *3*(6), 854–864. https://doi.org/10.1109/JIOT.2016.2584538

Chong, Z. J., Qin, B., Bandyopadhyay, T., Wongpiromsarn, T., Rebsamen, B., Dai, P., Kim, S., Jr, M., Hsu, D., Rus, D., and Frazzoli, E. (2012). Autonomy for Mobility on Demand. *2012 IEEE/RSJ International Conference on Intelligent Robots and Systems.*, 4235–4236. https://doi.org/10.1109/IROS.2012.6386287

Christi, W. (2017). *Corporate Surveillance in Everyday Life: How Companies Collect, Combine, Analyze, Trade and Use Personal Data on Billions*. https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf

Christopher Niesche. (2019, August 13). Big data centres on regional areas. *Australian Financial Review*. https://www.afr.com/companies/professional-services/big-data-centres-on-regional-areas-20190811-p52g0m

City of Melbourne. (2016). *BigBelly bin trial a success*. https://www.melbourne.vic.gov.au/news-and-media/Pages/bigbelly-bin-trial-a-success.aspx

City of Newcastle. (2017). *Newcastle City Council: Smart City Strategy 2017-2021*. https://www.newcastle.nsw.gov.au/getmedia/392db4be-d418-48d8-a593-7a17a4b482bb/2752_Smart-City-Strategy-FINAL-WEB.aspx

Clarke, R., and Greenleaf, G. (2017). Dataveillance regulation: A research framework. *Journal of Law, Information and Science*, *25*(1), 104.

Clarke, R., Heitlinger, S., Light, A., Forlano, L., Foth, M., and Disalvo, C. (2019). More-than-human participation: Design for sustainable smart city futures. *Interactions*, *26*, 60–63. https://doi.org/10.1145/3319075

COAG Energy Council. (2020). *Energy Security Board*. http://www.coagenergycouncil.gov.au/market-bodies/energy-security-board

Cohen, B. (2015). *The 3 Generations of Smart Cities*. Fast Company. https://www.fastcompany.com/3047795/the-3-generations-of-smart-cities

Cohen, N. (2015). Continuous glucose monitoring and pumps. *Australian Family Physician*, *44*, 284–287. http://www.racgp.org.au/afp/2015/may/continuous-glucose-monitoring-and-pumps/

Consumer Reports. (2018). *Samsung and Roku Smart TVs Vulnerable to Hacking, Consumer Report Finds*. Consumer Reports. https://www.consumerreports.org/televisions/samsung-roku-smart-tvs-vulnerable-to-hacking-consumer-reports-finds/

Cook, G., Lee, J., Tsai, T., Kong, A., Deans, J., Johnson, B., and Jardim, E. (2017). Clicking Clean: Who is winning the race to build a Green Internet? *Greenpeace Inc., Washington, DC*, 1–102.

Correa, D. (2016). IoT lightbulb worm takes over all smart lights until entire city is infected. *SC Media: The Cybersecurity Source*. https://www.scmagazineuk.com/iot-lightbulb-worm-takes-smart-lights-until-entire-city-infected/article/1475933

Coulson, S., Woods, M., Scott, M., and Hemment, D. (2018). Making Sense: Empowering participatory sensing with transformation design. *The Design Journal*, *21*(6), 813–833. https://doi.org/10.1080/14606925.2018.1518111

Crabtree, A., Lodge, T., Colley, J., Greenhalgh, C., Glover, K., Haddadi, H., Amar, Y., Mortier, R., Li, Q., Moore, J., Wang, L., Yadav, P., Zhao, J., Brown, T., Urquhart, L., and McAuley, D. (2018). Building accountability into the Internet of Things: the IoT Databox model. *Journal of Reliable Intelligent Environments*, *4*. https://doi.org/10.1007/s40860-018-0054-5

Crist, P., Greer, E., Ratti, C., Humanes, P., Konzett, G., Tijing, J., Figuero, D., and Lax, R. (2015). *Big Data and Transport: Understanding and assessing the options*. https://www.itf-oecd.org/sites/default/files/docs/15cpb_bigdata_0.pdf

Critical Comms. (2019). *Communication above the clouds*. https://www.criticalcomms.com.au/content/industry/article/communications-above-the-clouds-736907554#axzz6H60ROyCp

Crozier, R. (2019, September 10). *NBN Co is building a user-facing technical field force*. ITnews. https://www.itnews.com.au/news/nbn-co-is-building-a-user-facing-technical-field-force-530789

CSIRO. (2013). *Change and choice: The Future Grid Forum's analysis of Australia's potential electricity pathways to 2050*. https://publications.csiro.au/rpr/download?pid=csiro:EP1312486&dsid=DS13

CSIRO. (2017). *Amazon Rainforest Biodiversity Monitoring.* https://research.csiro.au/dss/amazon-rainforest-biodiversity-monitoring/

CSIRO. (2020). *A dry landscape and a dire season: we explain the current bushfire environment*. https://blog.csiro.au/explain-current-bushfire-environment/

CurtinX. (2019). *MicroMasters Program in Internet of Things (IoT)*. https://www.edx.org/micromasters/curtinx-internet-of-things-iot

Da Xu, L., He, W., and Li, S. (2014). Internet of things in industries: A survey. *IEEE Transactions on Industrial Informatics*, *10*(4), 2233–2243.

Dang, L. M., Min, K., Han, D., Jalil Piran, M., and Moon, H. (2019). *A Survey on Internet of Things and Cloud Computing for Healthcare*. *8*. https://doi.org/10.3390/electronics8070768

Davies, J. (2018, October 8). Thinking Ahead To Society 5.0. *Semiconductor Engineering*. https://semiengineering.com/thinking-ahead-to-society-5-0/

Deloitte LLP. (2018). *A journey through the FCA regulatory sandbox: The benefits, challenges, and next steps*. https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/financial-services/deloitte-uk-fca-regulatory-sandbox-project-innovate-finance-journey.pdf

Department of Communications and the Arts. (2017). *5G - Enabling the future economy*. https://www.communications.gov.au/departmental-news/5g-enabling-future-economy

Department of Communications and the Arts. (2019). *Online Safety Legislative Reform: Discussion Paper December 2019*. https://www.communications.gov.au/have-your-say/consultation-new-online-safety-act

Department of Education, Skills and Employment. (2020). *Regional University Centres (formerly known as Regional Study Hubs)*. https://www.education.gov.au/regional-university-centres-formerly-known-regional-study-hubs

Department of Education, Skills and Employment, and Education Services Australia. (2016). *Digital Technologies Hub*. https://www.digitaltechnologieshub.edu.au/

Department of Foreign Affairs and Trade. (2019). *Australia's Top 10 Goods & Services Exports and Imports (2018)*. https://dfat.gov.au/trade/resources/trade-at-a-glance/Pages/top-goods-services.aspx

Department of Homeland Security's Cybersecurity and Infrastructure Security Agency. (2020). *ICS Medical Advisory (ICSMA-19-080-01). Medtronic Conexus Radio Frequency Telemetry Protocol (Update A)*. Medtronic Conexus Radio Frequency Telemetry Protocol. https://www.us-cert.gov/ics/advisories/ICSMA-19-080-01

Department of Infrastructure, Transport, Regional Development and Communications. (2020a). *Consultation on a new Digital Technology Hub*. https://www.communications.gov.au/have-your-say/consultation-new-digital-technology-hub

Department of Infrastructure, Transport, Regional Development and Communications. (2020b). *Mobile Black Spot Program*. https://www.communications.gov.au/what-we-do/phone/mobile-services-and-coverage/mobile-black-spot-program

Department of Infrastructure, Transport, Regional Development and Communications. (2020c). *Regional Connectivity Program*. https://www.communications.gov.au/what-we-do/internet/regional-connectivity-program

Department of Infrastructure, Transport, Regional Development and Communications. (2020d). *Universal Service Guarantee for telecommunications*. https://www.communications.gov.au/what-we-do/phone/phone-services/universal-service-guarantee-telecommunications

Department of the Prime Minister and Cabinet. (2020). *User guide to the Australian Government Guide to Regulatory Impact Analysis*. https://www.pmc.gov.au/sites/default/files/publications/user-guide-ria.pdf

Desai, P., Sheth, A., and Anantharam, P. (2015). *Semantic Gateway as a Service architecture for IoT Interoperability*. https://doi.org/10.1109/MobServ.2015.51

Dettmer, A., and Wieladek, A. (2019). *Australia Rebooted*.

Deursen, A. J. A. M., Zeeuw, A., de Boer, P., Jansen, G., and Van Rompay, T. (2019). Digital inequalities in the Internet of Things: differences in attitudes, material access, skills, and usage. *Information, Communication & Society*, 1–19. https://doi.org/10.1080/1369118X.2019.1646777

Dia, H. (2017). *Low carbon mobility for future cities: principles and applications*.

Dia, H., Abduljabbar, R., and Liyanage, S. (2019). *Smart Mobility: Unlocking the Value of the Internet of Things*.

Discher, G., and Ponder, J. (2019, July 24). *IoT Update: Federal Lawmakers Focus on Smart Cities*. Lexology. https://www.lexology.com/library/detail.aspx?g=4abc8a2d-ea78-49fe-b91f-19e3b3c775c1

Dolman, G. (2019). *Key road safety data update*. https://acrs.org.au/wp-content/uploads/2019/11/Dolman-BITRE-Stakeholder_roadsafety_roundtable_2Sept2019-final.pdf

Domestic Violence Resource Centre Victoria. (2019). *Legal Guides*. https://www.dvrcv.org.au/knowledge-centre/legal-protection-safety/legal-guides

Dua, A., and Anderson, C. (2013). *Wire Rope Barrier Monitoring System (Load cell communication) - An overview*. https://acrs.org.au/files/papers/10 Dua_PR.pdf

Duke, J. (2019). A “regional 5G divide”: Telcos tipped to share mobile towers in country areas. *Sydney Morning Herald*. https://www.smh.com.au/business/companies/a-regional-5g-divide-telcos-tipped-to-share-mobile-towers-in-country-areas-20191125-p53dy3.html

Dunbar, R. (2016). Do online social media cut through the constraints that limit the size of offline social networks? *Royal Society Open Science*, *3*, 150292. https://doi.org/10.1098/rsos.150292

Echo Kids Privacy. (2019). *Kid Skills Privacy Analysis*. Echo Kids Privacy. https://www.echokidsprivacy.com/

Elkhodr, M., Shahrestani, S., and Cheung, H. (2016). Emerging Wireless Technologies in the Internet of Things: A Comparative Study. *International Journal of Wireless & Mobile Networks*, *8*. https://doi.org/10.5121/ijwmn.2016.8505

Ellis, J. (2019, July 23). What’s Happening With Markups for the IoT Cybersecurity Improvement Act of 2019. *Rapid7*. https://blog.rapid7.com/2019/07/23/whats-happening-with-markups-for-the-iot-cybersecurity-improvement-act-of-2019/

Energy Networks Australia & CSIRO. (2017). *Electricity Network Transformation Roadmap: Final Report*. http://www.energynetworks.com.au/assets/uploads/entr_final_report_april_2017.pdf

Ericsson. (2019). *Ericsson Mobility Report November 2019*. https://www.ericsson.com/4acd7e/assets/local/mobility-report/documents/2019/emr-november-2019.pdf

Etherington, D. (2020). *SpaceX launches 58 more Starlink satellites and 3 Planet Skysats for first rideshare launch*. Tech Crunch. https://techcrunch.com/2020/06/13/spacex-launches-58-more-starlink-satellites-and-3-planet-skysats-for-first-rideshare-launch/

Eubanks, V. (2018). *Automating Inequality: How high-tech tools profile, police, and punish the poor*. St. Martin’s Press.

European Commission. (2016). *Staff Working Document: “Advancing the Internet of Things in Europe”, accompanying the document “Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016SC0110

European Commission. (2017). *Values and ethics in Innovation for Responsible Technology in EUrope*. https://cordis.europa.eu/project/id/732027

European Commission. (2019). *Research & Innovation in Internet of Things*. https://ec.europa.eu/digital-single-market/en/research-innovation-iot

European Telecommunications Standards Institute. (2019). *ETSI TR 103 582 V1.1.1 (2019-07) Technical Report: EMTEL; Study of use cases and communications involving IoT devices in provision of emergency situations*. https://www.etsi.org/deliver/etsi_tr/103500_103599/103582/01.01.01_60/tr_103582v010101p.pdf

European Union Agency for Cybersecurity. (2020). *ENISA Good practices for IoT and Smart Infrastructures Tool*.

Evensen, H., Gribb, M., and Nasiri, A. (2019). Internet of Things Curriculum Workshop: An Interdisciplinary, Cross-Institutional Effort for Education in an Expanding Field. *2019 ASEE Annual Conference & Exposition*.

Expert Group on Liability and New Technologies - New Technologies Formation. (2019). *Liability for Artificial Intelligence and other emerging digital technologies*. https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=36608

Fagnant, D., and Kockelman, K. (2015). Preparing a nation for autonomous vehicles: Opportunities, barriers and policy recommendations. *Transportation Research Part A: Policy and Practice*, *77*. https://doi.org/10.1016/j.tra.2015.04.003

Fairweather, N. (2017). *Surveillance in Employment: The Case of Teleworking* (pp. 381–391). https://doi.org/10.4324/9781315259697-37

Fang, Y., Chau, A., Fung, H., and Woo, J. (2019). Loneliness Shapes the Relationship between Information and Communications Technology Use and Psychological Adjustment among Older Adults. *Gerontology*, 1–9. https://doi.org/10.1159/000495461

Farahani, B., Firouzi, F., Chang, V., Badaroglu, M., Constant, N., and Mankodiya, K. (2017). Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare. *Future Generation Computer Systems*. https://doi.org/10.1016/j.future.2017.04.036

Färber, F., Cha, S. K., Primsch, J., Bornhövd, C., Sigg, S., and Lehner, W. (2012). SAP HANA database: data management for modern business applications. *ACM Sigmod Record*, *40*(4), 45–51.

Farbotko, C. (2018). *Domestic Environmental Labour: An Ecofeminist Perspective on Making Homes Greener*. Routledge. https://doi.org/10.4324/9781315772455

Financial Conduct Authority. (2019). *The Impact and Effectiveness of Innovate*. https://www.fca.org.uk/publication/research/the-impact-and-effectiveness-of-innovate.pdf

FindAMasters. (2019). *Internet of Things search*. https://www.findamasters.com/masters-degrees/?Keywords=internet+of+things

Flammini, A., Ferrari, P., Marioli, D., Sisinni, E., and Taroni, A. (2009). Wired and Wireless Sensor Networks for Industrial Applications. *Microelectron. J.*, *40*(9), 1322–1336. https://doi.org/10.1016/j.mejo.2008.08.012

Flore, D. (2017). *5G-NR workplan for eMBB*. 3GPP. https://www.3gpp.org/news-events/3gpp-news/1836- 5g_nr_workplan

Forbes. (2018, December 4). How Japan Is Harnessing IoT Technology To Support Its Aging Population. *Forbes*. https://www.forbes.com/sites/japan/2018/12/04/how-japan-is-harnessing-iot-technology-to-support-its-aging-population/#628ea9673589

ForbrukerRadet (Norwegian Consumer Council). (2016). *Connected toys violate European consumer law*. ForbrukerRadet (Norwegian Consumer Council). https://www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws

Forlano, L. (2016). Decentering the Human in the Design of Collaborative Cities. *Design Issues*, *32*, 42–54. https://doi.org/10.1162/DESI_a_00398

Forti, V., Baldé, C. P., Kuehr, R., and Bel, G. (2020). *The Global E-waste Monitor 2020: Quanties, flows and the circular economy potential*. http://ewastemonitor.info/wp-content/uploads/2020/07/GEM_2020_def_july1_low.pdf#.

Foth, M. (2016). *Early experiments show a smart city plan should start with people first*. The Conversation. https://theconversation.com/early-experiments-show-a-smart-city-plan-should-start-with-people-first-60174

Foth, M. (2017). The next urban paradigm: Cohabitation in the smart city. *It - Information Technology*, *59*. https://doi.org/10.1515/itit-2017-0034

Foth, M. (2018). Participatory urban informatics: towards citizen-ability. *Smart and Sustainable Built Environment*, *7*, 0. https://doi.org/10.1108/SASBE-10-2017-0051

Foth, M., Hudson-Smith, A., and Gifford, D. (2016). Smart Cities, Social Capital, and Citizens at Play: A Critique and A Way Forward. In F. X. Olleros & M. Zhegu (Eds.), *Research Handbook on Digital Transformations* (pp. 203–222). Edward Elgar Publishing. https://doi.org/10.4337/9781784717766.00017

Fowler, E. (2019). Evergen touts "largest" virtual power plant. *Australian Financial Review*.

Franceschi-Bicchierai, L. (2016). *A GPS Tracker for Kids Had a Bug That Would Let Hackers Stalk Them*. Motherboard, Tech by Vice. https://www.vice.com/en_us/article/bmvnzz/a-gps-tracker-for-kids-had-a-bug-that-would-let-hackers-stalk-them

Frankel, T. C. (2016). The Cobalt Pipeline: Tracing the path from deadly hand-dug mines in Congo to consumers phones and laptops. *The Washington Post*. https://www.washingtonpost.com/graphics/business/batteries/congo-cobalt-mining-for-lithium-ion-battery/

Fredericks, J., Caldwell, G., Foth, M., and Tomitsch, M. (2019). *The City as Perpetual Beta: Fostering Systemic Urban Acupuncture: Digital Media and Collaborative City-Making in the Network Society* (pp. 67–92). https://doi.org/10.1007/978-981-13-2694-3_4

Frey, C. B., and Osborne, M. A. (2013). *The Future of Employment: How Susceptible are Jobs to Computerisation*. www.oxfordmartin.ox.ac.uk/downloads/academic/The_Future_of_Employment.pdf

Frias, J., Virdi, N., Raja, P., Kim, Y., Savage, G., and Osterberg, L. (2017). Effectiveness of Digital Medicines to Improve Clinical Outcomes in Patients with Uncontrolled Hypertension and Type 2 Diabetes: Prospective, Open-Label, Cluster-Randomized Pilot Clinical Trial. *Journal of Medical Internet Research*, *19*, e246. https://doi.org/10.2196/jmir.7833

Funk, A. (2020). Fighting Covid-19 Shouldn't Mean Abandoning Human Rights. *Wired*. https://www.wired.com/story/opinion-fighting-covid-19-shouldnt-mean-abandoning-human-rights/

Gabrys, J. (2014). Programming environments: Environmentality and Citizen Sensing in the Smart City. *Environment and Planning D: Society and Space*, *32*, 30–48. https://doi.org/10.1068/d16812

Gao, Z., and Kornhauser, M. (2014). Uncongested Mobility for All: A Proposal for an Area Wide Autonomous Taxi System in New Jersey. *Transportation Research Board 93rd Annual Meeting*.

Geoscience Australia. (2019). *Positioning Australia*. https://www.ga.gov.au/scientific-topics/positioning-navigation/positioning-australia

Global Mobile Suppliers Association. (2019). *Narrow Band IoT & M2M - Global Narrowband IoT – LTE-M networks – March 2019*. https://gsacom.com/paper/global-narrowband-iot-lte-m-networks-march-2019/

Goode, A., Reeves, M., Owen, N., and Eakin, E. (2013). Results from the dissemination of a telephone-delivered intervention for healthy lifestyle and weight loss: The Optimal Health Program. *Translational Behavioral Medicine*, *3*, 340–350. https://doi.org/10.1007/s13142-013-0210-7

Goode, L. (2018, February). Facial recognition software is biased towards white men, researcher finds. *The Verge2*. https://www.theverge.com/2018/2/11/17001218/facial-recognition-software-accuracy-technology-mit-white-men-black-women-error

Goodin, D. (2017, February 28). Creepy IoT teddy bear leaks >2 million parents' and kids' voice messages. *Ars Technica*. https://arstechnica.com/information-technology/2017/02/creepy-iot-teddy-bear-leaks-2-million-parents-and-kids-voice-messages/

Goodman, E., and Powles, J. (2019). Urbanism Under Google: Lessons from Sidewalk Toronto. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3390610

Gossart, C. (2015). *Rebound Effects and ICT: A Review of the Literature* (Vol. 310). https://doi.org/10.1007/978-3-319-09228-7_26

Gray, C., Ayre, R., Hinton, K., and Tucker, R. S. (2015). Power consumption of IoT access network technologies. *2015 IEEE International Conference on Communication Workshop (ICCW)*, 2818–2823.

Greenberg, A. (2015). *Hackers Remotely Kill a Jeep on the Highway - With Me in It*. Wired. https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Greenleaf, G. (2014). *Privacy Enforcement in Australia is Strengthened: Gaps Remain*.

Griffith, C. (2018, June 27). The different ways we learn pose a challenge in the age of AI. *The Australian*.

Grind, K., McMillen, R., and Wilde Matthews, A. (2020). To Track Virus, Governments Weigh Surveillance Tools That Push Privacy Limits; Geolocation and facial-recognition systems can locate vectors of infections, but they also gather highly personal data. *Wall Street Journal (Online)*. https://www.wsj.com/articles/to-track-virus-governments-weigh-surveillance-tools-that-push-privacy-limits-11584479841

GSMA. (2018). *Opportunities in the IoT: Evolving roles for mobile operators*. https://www.gsma.com/iot/wp-content/uploads/2018/09/New-Roles-for-Operators-in-the-IoT-k.pdf

Gunasekara, G. (2020). *Does COVID-19 justify the suspension of privacy?* https://www.auckland.ac.nz/en/news/2020/03/26/does-covid-19-justify-the-suspension-of-privacy-.html

Halliday, J., and Lam, R. (2015). Internet of Things: Just Hype or the Next Big Thing? Part I. *Communications Law Bulletin*, *34*(4), 6–7. http://www.austlii.edu.au/au/journals/CommsLawB/2015/14.html

Halliday, J., and Lam, R. (2016). Internet of Things: Just Hype of the Next Big Thing? Part II. *Communications Law Bulletin*, *34*(4), 6–7. http://www.austlii.edu.au/au/journals/CommsLawB/2016/2.pdf

Hansen, A. (2020). *Factory of the Future's innovative take on digital twins*. Swinburne University of Technology News. https://www.swinburne.edu.au/news/latest-news/2020/01/factory-of-the-futures-innovative-take-on-digital-twins.php

Hargreaves, T., and Wilson, C. (2017). *Smart Homes and Their Users*. Springer Cham.

Hearn, P. (2018, November 12). New Hampshire judge tells Amazon to turn over Echo recordings in murder case. *Digital Trends*. https://www.digitaltrends.com/news/alexa-court-new-hampshire-judge-requests-echo-recordings/

Heuss, K. (2014). *Is IoT the new Y2K?* ZDNet. https://www.zdnet.com/article/is-iot-the-new-y2k/

Higgenbotham, S. (2018). *The Internet of Trash: IoT Has a Looming E-Waste Problem*. IEEE Spectrum. https://spectrum.ieee.org/telecom/internet/the-internet-of-trash-iot-has-a-looming-ewaste-problem

Hilty, L., Som, C., and Koehler, A. (2004). Assessing the Human, Social, and Environmental Risks of Pervasive Computing. *Human and Ecological Risk Assessment*, *10*. https://doi.org/10.1080/10807030490513874

Hirsch-Kreinsen, H. (2016). Digitization of industrial work: development paths and prospects. *Journal for Labour Market Research*, *49*. https://doi.org/10.1007/s12651-016-0200-6

Hogan Lovells. (2019). *A comparison of IoT regulatory uncertainty in the EU, China, and the United States*. https://www.hoganlovells.com/en/publications/a-comparison-of-iot-regulatory-uncertainty-in-the-eu-china-and-the-united-states

Holland, P., and Bardoel, E. (2016). The impact of technology on work in the twenty-first century: exploring the smart and dark side. *The International Journal of Human Resource Management*, *27*, 1–3. https://doi.org/10.1080/09585192.2016.1238126

Holland, P., Cooper, B., and Hecker, R. (2019). *Social Media at Work: A New Form of Employee Voice?* (pp. 73–89). https://doi.org/10.1007/978-981-13-2820-6_4

Huawei Technologies Co. Ltd. (2016). *5G network architecture, a high-level perspective*. https://www.huawei.com/minisite/hwmbbf16/insights/5G-Nework-Architecture-Whitepaper-en.pdf

Hung, M. (2017). *Leading the IoT Gartner Insights on How to Lead in a Connected World*. https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf

IARC. (2013). Non-ionizing radiation, Part 2: Radiofrequency electromagnetic fields. *Iarc Monographs on the Evaluation of Carcinogenic Risks to Humans*, *102*, 1–460. https://monographs.iarc.fr/wp-content/uploads/2018/06/mono102.pdf

IBM Analytics. (2015). *IBM Point of View: Internet of Things Security*. https://www.industryofthingsvoice.com/wp-content/uploads/2017/10/IBM-Point-of-View-IoT-Security.pdf

IDC. (2019). *IDC Forecasts Worldwide Technology Spending on the Internet of Things to Reach $1.2 Trillion in 20202*. http://web.archive.org/web/20190530144315/https://www.idc.com/getdoc.jsp?containerId=prUS43994118

Information Commissioner's Office. (2018). *Actions We've Taken*. https://ico.org.uk/action-weve-taken/enforcement/

Infrastructure Australia. (2019). *Australian Infrastructure Audit 2019: Telecommunications*. https://www.infrastructureaustralia.gov.au/sites/default/files/2019-08/Australian Infrastructure Audit 2019 - 8. Telecommunications.pdf

Iniguez, G., Govezensky, T., Dunbar, R., Kaski, K., and Barrio, R. (2014). Effects of deception in social networks. *Proceedings of the Royal Society B: Biological Sciences*, *281*, 20141195. https://doi.org/10.1098/rspb.2014.1195

Innovation and Science Australia. (2017). *Australia 2030: Prosperity through innovation*. Australian Government, Canberra. https://industry.gov.au/Innovation-and-Science-Australia/Documents/Australia-2030-Prosperity-through-Innovation-Full-Report.pdf

Institute for Public Policy Research. (2015). *Technology, globalisation and the future of work in Europe: Essays on employment in a digitised economy* (T. Dolphin (ed.)). https://www.ippr.org/files/publications/pdf/technology-globalisation-future-of-work_Mar2015.pdf?noredirect=1

Intel. (2019). *Smart Energy for a more Efficient and Sustainable World*. https://www.intel.com.au/content/www/au/en/energy/energy-overview.html

International Commission on Non-Ionizing Radiation Protection (ICNIRP). (2020). *ICNIRP Guidelines for Limiting Exposure to Electromagnetic Fields (100 kHz to 300 GHz)*. https://www.icnirp.org/cms/upload/publications/ICNIRPrfgdl2020.pdf

Internet of Things Alliance Australia. (2017a). *Good Data Practice: A Guide for Business to Consumer Interest of Things Services for Australia V1.0*. http://www.iot.org.au/wp/wp-content/uploads/2016/12/Good-Data-Practice-A-Guide-for-B2C-IoT-Services-for-Australia-Nov-2017.pdf

Internet of Things Alliance Australia. (2017b). *Internet of Things: Security Guideline*. https://www.iot.org.au/wp/wp-content/uploads/2016/12/IoTAA-Security-Guideline-V1.2.pdf

Internet of Things Alliance Australia. (2017c). *IoT and Government's Role in the Development of Cities: Submission to the Standing Committee on Infrastructure, Transport and Cities*. file:///C:/Users/StephanieChan/Downloads/IoTAA Submission to Inquiry - Australian Government's Role in the Development of Cities.pdf

Internet of Things Alliance Australia. (2017d). *Strategic Plan to Strengthen IoT in Australia*. http://www.iot.org.au/wp/wp-content/uploads/2016/12/IoTAA-Strategic-Plan-to-Strengthen-IoT-Security-in-Australia-v4.pdf

Internet of Things Alliance Australia. (2019). *"State of Nation" Briefing Report*. https://www.iotimpact.com.au/iot-state-of-the-nation

Internet Society. (2019). *Solutions for Traffic Backhaul in Community Networks*. https://www.internetsociety.org/wp-content/uploads/2019/11/Backhaul-Solutions-Fact-Sheet.pdf

Intouch Magazine. (2019). Newcastle Leads the Way with Smart City Infrastructure. *Intouch Magazine*. https://www.intouchmagazine.com.au/single-post/2019/11/01/Newcastle-Leads-the-Way-with-Smart-City-Infrastructure

Ion, M., Kreuter, B., Nergiz, E., Patel, S., Saxena, S., Seth, K., Shanahan, D., and Yung, M. (2017). *Private Intersection-Sum Protocol with Applications to Attributing Aggregate Ad Conversions*. https://eprint.iacr.org/2017/738

IoT4SMEs. (2019). *Internet of Things for European Small and Medium Enterprises*. https://www.iot4smes.eu/en/default.aspx

Iridum. (2019). *Iridum Completes Historic Satellite Launch Campaign*. http://investor.iridium.com/2019-01-11-Iridium-Completes-Historic-Satellite-Launch-Campaign

ITS Australia. (2018). *Mobility as a Service in Australia: Customer insights and opportunities*.

ITU. (2020). *ITU EMF Guide*. http://emfguide.itu.int/emfguide.html

Jalali, F., Hinton, K., Ayre, R., Alpcan, T., and Tucker, R. S. (2016). Fog computing may help to save energy in cloud computing. *IEEE Journal on Selected Areas in Communications*, *34*(5), 1728–1739.

James, S., Abate, D., Abate, K., Abay, S., Cristiana, A., Abbasi, N., Abbastabar, H., Abd-Allah, F., Abdela, J., Abdelalim, A., Abdollahpour, I., Suliankatchi, R., Abebe, Z., Abera, S., Zewdie, O., Niguse, H., Abu-Raddad, L., and Abu-Rmeileh, N. (2018). *Global, regional, and national incidence, prevalence, and years lived with disability for 354 diseases and injuries for 195 countries and territories, 1990–2017: a systematic analysis for the Global Burden of Disease Study 2017*.

Janakiram MSV. (2019, July 5). NVIDIA Brings Affordable GPU to the Edge with Jetson Nano. *The New Stack*. https://thenewstack.io/nvidia-brings-affordable-gpu-to-the-edge-with-jetson-nano/

Japanese Ministry of Economy, Trade and Investment. (2016, April 28). *METI Signed a Joint Statement Regarding Japan-Germany Cooperation on IoT/ Industrie 4.0*. https://www.meti.go.jp/english/ press/2016/0428_04.html

Jenkins, R. (2016). *Cyberwarfare as Ideal War* (pp. 89–114). https://doi.org/10.1093/ acprof:oso/9780190221072.003.0006

Johnston, M. (2019). *Melbourne Uni connects +700 apps in smart campus drive*. Itnews. https://www.itnews. com.au/news/melbourne-uni-connects-700-apps-in-smart-campus-drive-522720

Jones, N. (2018). How to stop data centres from gobbling up the world's electricity. *Nature*, *561*, 163–166. https://doi.org/10.1038/d41586-018-06610-y

Kakria, P., Tripathi, N., and Kitipawong, P. (2015). A Real-Time Health Monitoring System for Remote Cardiac Patients Using Smartphone and Wearable Sensors. *International Journal of Telemedicine and Applications*, *2015*, 1–11. https://doi.org/10.1155/2015/373474

Kamilaris, A., and Ostermann, F. (2018). Geospatial Analysis and the Internet of Things. *ISPRS International Journal of Geo-Information*, *7*, 269. https://doi. org/10.3390/ijgi7070269

Karipidis, K., Henderson, S., Wijayasinghe, D., Tjong, L., and Tinker, R. (2017). Exposure to Radiofrequency Electromagnetic Fields From Wi-Fi in Australian Schools. *Radiation Protection Dosimetry*, *175*. https:// doi.org/10.1093/rpd/ncw370

Karvonen, A., Cugurullo, F., and Caprotti, F. (2019). Introduction: situating smart cities. In A. Karvonen, F. Cugurullo, & F. Caprotti (Eds.), *Inside Smart Cities: Place, Politics and Urban Innovation* (pp. 19–30). Routledge.

Katz, C., Meadows, J., Aradi, L., and Mathis, P. (2017). *Recent IoT Device Cases*. https://www.crowelldatalaw. com/2017/07/recent-iot-device-cases/

Kennedy, D. (2018). *5G in Australia - Evolution not Revolution*. https://www.nbnco.com.au/content/dam/ nbnco2/2018/documents/media-centre/5G_report_ June_2018.pdf

Khan, M., Aubet, F.-X., Pahl, M.-O., and Härri, J. (2019). *Deep Learning-aided Application Scheduler for Vehicular Safety Communication*.

Khanal, S., Lloyd, B., Rissel, C., Portors, C., Grunseit, A., Indig, D., Ibrahim, I., and McElduff, S. (2016). Evaluation of the implementation of Get Healthy at Work, a workplace health promotion program in New South Wales, Australia. *Health Promotion Journal of Australia : Official Journal of Australian Association of Health Promotion Professionals*, *27*. https://doi.org/10.1071/ HE16039

Kim, S.-S., Chung, Y., Perry, M., Kawachi, I., and Subramanian, S. (2012). Association between Interpersonal Trust, Reciprocity, and Depression in South Korea: A Prospective Analysis. *PloS One*, *7*, e30602. https://doi.org/10.1371/journal.pone.0030602

Kitchin, R. (2013). The Real-Time City? Big Data and Smart Urbanism. *SSRN Electronic Journal*. https://doi. org/10.2139/ssrn.2289141

Klein, G., Elphinstone, K., Heiser, G., Andronick, J., Cock, D., Derrin, P., Elkaduwe, D., Engelhardt, K., Kolanski, R., and Norrish, M. (2009). seL4: Formal verification of an OS kernel. *Proceedings of the ACM SIGOPS 22nd Symposium on Operating Systems Principles. ACM*.

Koehler, A., and Erdmann, L. (2004). Expected Environmental Impacts of Pervasive Computing. *Human and Ecological Risk Assessment: An International Journal*, *10*(5). https://doi. org/10.1080/10807030490513856

Koh, D. (2020a). *SPHCC employs IoT tech and wearable sensors to monitor COVID-19 patients*.

Koh, D. (2020b). *Temp Pal smart thermometer helps reduce COVID-19 spread in hospitals*. Mobihealthnews.

Korom, P. (2019). A bibliometric visualization of the economics and sociology of wealth inequality: a world apart? *Scientometrics*, *118*. https://doi. org/10.1007/s11192-018-03000-z

Korzun, D. (2017). *Internet of Things Meets Mobile Health Systems in Smart Spaces: An Overview* (pp. 111–129). https://doi.org/10.1007/978-3-319-49736-5_6

Kovács-Ondrejkovic, O., Strack, R., Antebi, P., López Gobernado, A., and Lyle, E. (2019, November 5). Decoding global trends in Upskilling and Reskilling. *BCG*.

Kovacs, E. (2014). *Hackers Attack Shipping and Logistics Firms Using Malware-Laden Handheld Scanners*. Security Week. https://www.securityweek.com/ hackers-attack-shipping-and-logistics-firms-using-malware-laden-handheld-scanners

Koziol, M. (2018). Now's the time to think about what comes after 5G: We need to make sure the backbone of every network can support future demands for data - [Spectral Lines]. *IEEE Spectrum*, *55*(12), 6. https:// doi.org/10.1109/MSPEC.2018.8544970

KPMG. (2018, March 20). *KPMG to boost headcount by 50% in Australia's leading IoT consulting practice*. https://news.efinancialcareers.com/au-en/308174/ kpmg-australia-internet-of-things-jobs-sc

Kshetri, N. (2017). The evolution of the internet of things industry and market in China: An interplay of institutions, demands and supply. *Telecommunications Policy*, *41*(1), 49–67. https://doi.org/https://doi. org/10.1016/j.telpol.2016.11.002

Kumar, P. M., Devi G, U., Manogaran, G., Sundarasekar, R., Chilamkurti, N., and Varatharajan, R. (2018). Ant colony optimization algorithm with Internet of Vehicles for intelligent traffic control system. *Computer Networks*, *144*, 154–162. https://doi.org/https://doi. org/10.1016/j.comnet.2018.07.001

Kurata, M., Kim, J., Lynch, J., Linden, G., Sedarat, H., Thometz, E., Hipley, P., and Sheng, L. (2012). Internet-Enabled Wireless Structural Monitoring Systems: Development and Permanent Deployment at the New Carquinez Suspension Bridge. *Journal of Structural Engineering*, *139*, 1688–1702. https://doi.org/10.1061/(ASCE)ST.1943-541X.0000609

Lacey, M., Lisaschuk, H., Giannopoulous, A., and Ogura, A. (2015a). *Shipping smarter: IoT opportunities in transport and logistics*. https://www2.deloitte.com/content/dam/insights/us/articles/iot-in-shipping-industry/DUP1271_IoT_Transportation-and-Logistics_MASTER.pdf

Lacey, M., Lisaschuk, H., Giannopoulous, A., and Ogura, A. (2015b). *Shipping smarter: IoT opportunities in transport and logistics*.

Lavric, A., and Popa, V. (2017). Internet of Things and LoRa™ Low-Power Wide-Area Networks: A survey. *2017 International Symposium on Signals, Circuits and Systems (ISSCS)*, 1–5. https://doi.org/10.1109/ISSCS.2017.8034915

Laykin, E. (2017). IoT Evidence Analysis and Preservation in Investigations and Litigation. *Conference Presentation, RSA Conference*. https://published-prd.lanyonevents.com/published/rsaus17/sessionsFiles/4839/LAW-W02-IoT-Evidence-Analysis-and-Preservation-in-Investigations-and-Litigation.pdf

Lee, E.-K., Gerla, M., Pau, G., Lee, U., and Lim, J.-H. (2016). Internet of Vehicles: From intelligent grid to autonomous cars and vehicular fogs. *International Journal of Distributed Sensor Networks*, *12*(9), 1550147716665500. https://doi.org/10.1177/1550147716665500

Leitão, R. (2018). Digital Technologies and their Role in Intimate Partner Violence. *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18*, 1–6. https://doi.org/10.1145/3170427.3180305

Leonard, P. (2017). *A Review of Australian Privacy Commissioner v Telstra Corporation Limited*. Gilbert + Tobin Lawyers. https://cdn.brandfolder.io/3RTTK3BV/as/pvy5d5-e7j9ug-ca5227/A_Review_of_Australian_Privacy_-_Commissioner_v_Telstra_Corporation_Limited.pdf

Leontidou, L. (2015). Smart Cities of the debt crisis: grassroots creativity in Mediterranean Europe. *Επιθεώρηση Κοινωνικών Ερευνών*, *144*(144), 69–101. http://dx.doi.org/10.12681/grsr.8626

Li, Z., Shahidehpour, M., and Liu, X. (2018). Cyber-secure decentralized energy management for IoT-enabled active distribution networks. *Journal of Modern Power Systems and Clean Energy*, *6*(5), 900–917. https://doi.org/10.1007/s40565-018-0425-1

Lindley, J., Coulton, P., and Alter, H. (2019). Networking with Ghosts in the Machine. Speaking to the Internet of Things. *The Design Journal*, *22*, 1187–1199. https://doi.org/10.1080/14606925.2019.1594984

Liu, T., and Ceder, A. (2015). Analysis of a new public-transport-service concept: Customized bus in China. *Transport Policy*, *39*, 63–76. https://doi.org/10.1016/j.tranpol.2015.02.004

Liyanage, S., Dia, H., Abduljabbar, R., and Bagloee, S. (2019). Flexible Mobility On-Demand: An Environmental Scan. *Sustainability*, *11*, 1262. https://doi.org/10.3390/su11051262

Lockie, S., Fairley-Grenot, K., Ankeny, R., Botterill, L., Howlett, B., McBratney, A., Probyn, E., Sorrell, T., Sukkarieh, S., and Woodhead, I. (2020). *The future of agricultural technologies.* www.acola.org

Loots, G. (2019). *Over 3 million new IoT "things" on our network*. https://exchange.telstra.com.au/over-3-million-new-iot-things-on-our-network/

LoRa Alliance. (2019, January 22). *LoRa Alliance Passes 100 LoRaWAN™ Network Operator Milestone with Coverage in 100 Countries*. https://lora-alliance.org/in-the-news/lora-alliance-passes-100-lorawantm-network-operator-milestone-coverage-100-countries

Lorinc, J. (2018). *A Mess on the Sidewalk*. The Baffler. https://thebaffler.com/salvos/a-mess-on-the-sidewalk-lorinc

Luusua, A., Ylipulli, J., and Rönkkö, E. (2017). Nonanthropocentric design and smart cities in the anthropocene. *It - Information Technology*, *59*. https://doi.org/10.1515/itit-2017-0007

Lyytinen, K., and Yoo, Y. (2002). Issues and challenges in ubiquitous computing. *Communications of the ACM*, *45*(12), 63–96. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.135.3184&rep=rep1&type=pdf

Ma, J., Yang, Y., Wei, G., Wang, F., Liu, T., Tu, W., and Song, C. (2017). Large Scale Demand Driven Design of a Customized Bus Network: A Methodological Framework and Beijing Case Study. *Journal of Advanced Transportation*, *2017*. https://doi.org/10.1155/2017/3865701

Manwaring, K. (2017a). Emerging information technologies: challenges for consumers. *Oxford University Commonwealth Law Journal*, *17*(2), 265–289. https://doi.org/10.1080/14729342.2017.1357357

Manwaring, K. (2017b). Kickstarting Reconnection: An Approach to Legal Problems Arising from Emerging Technologies. *Deakin Law Review*, *22*, 53–84. https://doi.org/10.21153/dlr2017vol22no1art722

Manwaring, K. (2018). Will Emerging Technologies Outpace Consumer Protection Law? The Case of Digital Consumer Manipulation. *Competition and Consumer Law Journal*, 141–181.

Manwaring, K., and Clarke, R. (2015). Surfing the third wave of computing: A framework for research into eObjects. *Computer Law & Security Review: The International Journal of Technology Law and Practice*, *31*, 586. https://doi.org/10.1016/j.clsr.2015.07.001

Manyika, J., Dobbs, R., Chui, M., Bughin, J., Bisson, P., and Woetzel, J. (2015). *The Internet of Things: Mapping the Value Beyond the Hype*. https://www.mckinsey.com/~/media/McKinsey/Industries/Technology Media and Telecommunications/High Tech/Our Insights/The Internet of Things The value of digitizing the physical world/The-Internet-of-things-Mapping-the-value-beyond-the-hype.ashx

Maras, M.-H. (2018, May 10). 4 ways 'internet of things' toys endanger children. *The Conversation*. https://theconversation.com/4-ways-internet-of-things-toys-endanger-children-94092

Maras, M.-H., and Wandt, A. (2019). Enabling mass surveillance: data aggregation in the age of big data and the Internet of Things. *Journal of Cyber Policy*, *4*, 1–18. https://doi.org/10.1080/23738871.2019.1590437

Marshall, A., Dale, A., Babacan, H., and Dezuanni, M. (2019). *Connectivity and digital inclusion in Far North Queensland's agricultural communities: Policy-focused report*. James Cook University. https://eprints.qut.edu.au/130869/

Martínez, J., Mejía, J., and Muñoz, M. (2016). Security analysis of the Internet of Things: A systematic literature review. *2016 International Conference on Software Process Improvement (CIMPS)*, 1–6. https://doi.org/10.1109/CIMPS.2016.7802809

Mathews-Hunt, K. (2017). *consumeR-IOT: where every thing collides. Promoting consumer internet of things protection in Australia*. Bond University.

Mattern, S. (2019). *The City Is Not a Computer* (pp. 133–142). https://doi.org/10.4324/9781315211633-15

McCauley, J., Buckalew, L., and Chung, G. (2015). *Internet of Things in Logistics: A collaborative report by DHL and Cisco on Implications and Use cases for the Logistics Industry*. https://discover.dhl.com/content/dam/dhl/downloads/interim/full/dhl-trend-report-internet-of-things.pdf

McEvoy, F. J. (2017). *Six Ethical Problems for Augmented Reality*. Becoming Human. https://becominghuman.ai/six-ethical-problems-for-augmented-reality-6a8dad27122

Mcgrath, S. (2019, January 21). Resolving IoT Security Issues with Blockchain Technology. *Hackernoon*. https://hackernoon.com/resolving-iot-security-issues-with-blockchain-technology-3ffb36357094

McKinsey & Company. (2019a). *Development in the mobility technology ecosystem - how can 5G help?* https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/development-in-the-mobility-technology-ecosystem-how-can-5g-help

McKinsey & Company. (2019b). *IOT Engineer - Operations*. https://www.mckinsey.com/careers/search-jobs/jobs/iotengineer-operations-22671

McNeill, D. (2015). Global firms and smart technologies: IBM and the reduction of cities. *Transactions of the Institute of British Geographers*, *40*. https://doi.org/10.1111/tran.12098

McRae, L., Ellis, K., and Kent, M. (2018). *The Internet of Things (IoT): Education and Technology The Relationship between education and technology for students with disabilities*. https://www.ncsehe.edu.au/wp-content/uploads/2018/02/IoTEducation_Formatted_Accessible.pdf

Mednis, A., Strazdins, G., Zviedris, R., Kanonirs, G., and Selavo, L. (2011). *Real Time Pothole Detection Using Android Smartphones with Accelerometers*. https://doi.org/10.1109/DCOSS.2011.5982206

Microsoft. (2019). *IoT Signals: Summary of Research Learnings 2019*. https://azure.microsoft.com/mediahandler/files/resourcefiles/iot-signals/IoT-Signals-Microsoft-072019.pdf

Milanés, V., Shladover, S., Spring, J., Nowakowski, C., Kawazoe, H., and Nakamura, M. (2014). Cooperative Adaptive Cruise Control in Real Traffic Situations. *Intelligent Transportation Systems, IEEE Transactions On*, *15*, 296–305. https://doi.org/10.1109/TITS.2013.2278494

Millard, C., Kuan Hon, W., and Singh, J. (2017). *Internet of Things Ecosystems: Unpacking Legal Relationships and Liabilities*. https://doi.org/10.1109/IC2E.2017.46

Minister for Communications, Cyber Safety and the Arts. (2020). *Strengthening telecommunications emergency resilience*. https://minister.infrastructure.gov.au/fletcher/media-release/strengthening-telecommunications-emergency-resilience

Minister for Education. (2019). *Applied technologies trial to be expanded nationally*. https://ministers.dese.gov.au/tehan/applied-technologies-trial-be-expanded-nationally-0

Minister for Families and Social Services. (2020). *Government supporting isolated older Australians during coronavirus*.

Minister for Health. (2020). *Building community confidence in 5G safety*. https://www.greghunt.com.au/building-community-confidence-in-5g-safety/

Mohanty, S. P., Choppali, U., and Kougianos, E. (2016). Everything you wanted to know about smart cities: The Internet of things is the backbone. *IEEE Consumer Electronics Magazine*, *5*(3), 60–70. https://doi.org/10.1109/MCE.2016.2556879

Monteiro, M. (2019). *Ruined by Design: How Designers Destroyed the World, and What We Can Do To Fix It*. Independently Published.

Moon, N., Baker, P., and Goughnour, K. (2019). Designing wearable technologies for users with disabilities: Accessibility, usability, and connectivity factors. *Journal of Rehabilitation and Assistive Technologies Engineering*, *6*, 205566831986213. https://doi.org/10.1177/2055668319862137

MOOvement. (2020). *The Network: Connect your whole property*. https://www.moovement.com.au/lora-network

Morabito, V. (2015). Managing Change for Big Data Driven Innovation. In *Big Data and Analytics* (pp. 125–153). Springer International Publishing. https://doi.org/10.1007/978-3-319-10665-6_7

Moradoff, N. (2009). Biometrics: Proliferation and constraints to emerging and new technologies. *Security Journal*, *23*(4), 276–298. https://doi.org/10.1057/sj.2008.21

Morley, J., Widdicks, K., and Hazas, M. (2018). Digitalisation, energy and data demand: The impact of Internet traffic on overall and peak electricity consumption. *Energy Research & Social Science*, *38*, 128–137. https://doi.org/https://doi.org/10.1016/j.erss.2018.01.018

Mu-Hyun, C. (2015, March 25). South Korea to invest $5b by 2020 in IoT and smart cars. *ZDNet*. https://www.zdnet.com/article/south-korea-to-invest-5b-by-2020-in-iot-and-smart-cars/

Mwaanga, P., Silondwa, M., Kasali, G., Paul, and Banda, M. (2019). Preliminary review of mine air pollution in Zambia. *Heliyon*, *5*. https://doi.org/10.1016/j.heliyon.2019.e02485

Naik, R., Macey, N., West, R., Godbehere, P., Thurston, S., Fox, R., Xiang, W., Kim, Y., Singh, I., Leadley, S., and DiCarlo, L. (2017). First Use of an Ingestible Sensor to Manage Uncontrolled Blood Pressure in Primary Practice: The UK Hypertension Registry. *Journal of Community Medicine & Health Education*, *07*. https://doi.org/10.4172/2161-0711.1000506

Nandimath, J., Banerjee, E., Patil, A., Kakade, P., Vaidya, S., and Chaturvedi, D. (2013). Big data analysis using Apache Hadoop. *2013 IEEE 14th International Conference on Information Reuse & Integration (IRI)*, 700–703.

National Grid. (2016). *Stakeholder Feedback document 2016: Future Energy Scenarios*.

National Transport Commission. (2019). *Automated Vehicle Program*. https://www.ntc.gov.au/sites/default/files/assets/files/NTC Automated Vehicle Reform Program Approach %28October 2019%29 - Public version.pdf

Nelson, P. (2019, January 17). Quantum-embedded chips could secure IoT. *Network World*. https://www.networkworld.com/article/3333808/quantum-embedded-chips-could-secure-iot.html

Nest Labs. (2015). *Energy Savings from the Nest Learning Thermostat: Energy Bill Analysis Results*. https://storage.googleapis.com/nest-public-downloads/press/documents/energy-savings-white-paper.pdf

Neumann, C. (2015). *Big data versus big congestion: using information to improve transport*.

Nguyen, A., Jabangwe, R., Paul, P., and Abrahamsson, P. (2017). *Security challenges in IoT development: a software engineering perspective*. https://doi.org/10.1145/3120459.3120471

Nguyen, P., and Solomon, L. (2018). *Consumer data and the digital economy: Emerging issues in data collection, use and sharing*.

Nicholls, L., Strengers, Y., and Tirado, S. (2017). *Smart home control. Exploring the potential for off-the-shelf enabling technologies in energy vulnerable and other households.*

Noble, S. (2018). *Algorithms of Oppression: How Search Engines Reinforce Racism*. https://doi.org/10.2307/j.ctt1pwt9w5

Nonnecke, B. M., Bruch, M., and Crittenden, C. (2016). *IoT and Sustainability: Practice, Policy and Promise Public Symposium*. https://escholarship.org/uc/item/7dp1t4p8

Noto La Diega, G., and Walden, I. (2016). Contracting for the "Internet of Things": Looking into the Nest. *European Journal of Law and Technology*, *7*(2).

Noura, M., Atiquzzaman, M., and Gaedke, M. (2019). Interoperability in Internet of Things: Taxonomies and Open Challenges. *Mobile Networks and Applications*, *24*(3), 796–809. https://doi.org/10.1007/s11036-018-1089-9

O'Donnell, L. (2018, August 13). Black Hat 2018: IoT Security Issues Will Lead to Legal 'Feeding Frenzy.' *Threatpost*. https://threatpost.com/black-hat-2018-iot-security-issues-will-lead-to-legal-feeding-frenzy/134997/

O'Keeffe, D., Salonidis, T., and Pietzuch, P. (2018). Frontier: resilient edge processing for the internet of things. *Proceedings of the VLDB Endowment*, *11*, 1178–1191. https://doi.org/10.14778/3231751.3231767

O'Malley, P., and Smith, G. (2019). *Disruption as distraction: Darwin's Smart City program, public resistance and the racialization of digital governance.*

O'Neil, C. (2016). *Weapons of math destruction: How big data increases inequality and threatens democracy.* https://www.amazon.com/Weapons-Math-Destruction-Increases-Inequality/dp/0553418815

Ochiai, H., Ishizuka, H., Kawakami, Y., and Esaki, H. (2011). A DTN-Based Sensor Data Gathering for Agricultural Applications. *IEEE Sensors Journal*, *11*(11), 2861–2868. https://doi.org/10.1109/JSEN.2011.2170562

OECD Global Forum on International Investment. (2002). *Foreign Direct Investment and the Environment: Lessons from the Mining Sector*. https://www.oecd.org/investment/investmentfordevelopment/34415091.pdf

Office of the Australian Information Commissioner. (2019a). *Australian Privacy Principles Guidelines: Privacy Act 1988*.

Office of the Australian Information Commissioner. (2019b). *Chapter B: Key Concepts*. https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-b-key-concepts/

Organisation for Economic Co-operation and Development. (2016). *The Internet of Things: Seizing the Benefits and Addressing the Challenges*. *252*. https://doi.org/https://doi.org/https://doi.org/10.1787/5jlwvzz8td0n-en

Organisation for Economic Co-operation and Development. (2018a). *IoT measurements and applications*. https://doi.org/10.1787/35209dbf-en

Organisation for Economic Co-operation and Development. (2018b). *Transformative technologies and jobs of the future*. https://www.oecd.org/innovation/transformative-technologies-and-jobs-of-the-future.pdf

Palmer, D. (2018). New IoT security rules: Stop using default passwords and allow software updates. *ZDNet*. https://www.zdnet.com/article/new-iot-security-rules-stop-using-default-passwords-and-allow-software-updates/

Pasquier, T., Singh, J., Powles, J., Eyers, D., Seltzer, M., and Bacon, J. (2017). Data provenance to audit compliance with privacy policy in the Internet of Things. *Springer Personal and Ubiquitous Computing*. https://doi.org/10.1007/s00779-017-1067-4

Petronio, S. (2002). *Boundary of Privacy: Dialetcis of Disclosure*. SUNY Press.

Plowman, R., Peters-Strickland, T., and Savage, G. (2018). Digital medicines: clinical review on the safety of tablets with sensors. *Expert Opinion on Drug Safety*, *17*. https://doi.org/10.1080/14740338.2018.1508447

Pooled Energy. (2020). *Pooled Energy: How it works*. https://pooledenergy.com.au/how-it-works/

PricewaterhouseCoopers, and Australian Computer Society. (2018). *Australia's IoT Opportunity: Driving Future Growth An ACS Report*. https://www.pwc.com.au/consulting/assets/publications/acs-pwc-iot-report-web.pdf

Prime Mover. (2019). *SCT Logistics trials asset use through Telstra monitoring*. Prime Mover Magazine.

Probst, A., Ebner, M., and Cox, J. (2018). Introducing Augmented Reality and Internet of Things at Austrian Secondary Colleges of Engineering. *International Conference on Interactive Collaborative Learning*, 3–12.

Productivity Commission. (2017). *Data Availability and Use*. https://www.pc.gov.au/inquiries/completed/data-access#report

PTC. (2019). *ThingWorx Platform Product Brief*. https://www.ptc.com/en/resources/iiot/product-brief/thingworx-platform

Pureswaran, V., and Brody, P. (2015). *Device democracy: Saving the future of the Internet of Thing*. https://www.ibm.com/downloads/cas/Y5ONA8EV

Qu, Z., Zhang, G., Cao, H., and Xie, J. (2017). LEO satellite constellation for Internet of Things. *IEEE Access*, *5*, 18391–18401.

Queensland Cardiovascular Group. (2017). *Remote Monitoring Service*. https://qcg.com.au/patients/remote-monitoring-service

Radatz, J., Geraci, A., and Katki, F. (1990). IEEE Standard Glossary of Software Engineering Terminology. In *IEEE Std 610.12-1990* (pp. 1–84). https://doi.org/10.1109/IEEESTD.1990.101064

Ray, P. P. (2018). A survey on Internet of Things architectures. *Journal of King Saud University - Computer and Information Sciences*, *30*(3), 291–319. https://doi.org/https://doi.org/10.1016/j.jksuci.2016.10.003

Redden, J., and Brand, J. (2019). *Data harm record*. https://datajusticelab.org/data-harm-record/

Rennie, E., Thomas, J., and Wilson, C. (2019). Aboriginal and Torres Strait Islander people and digital inclusion: what is the evidence and where is it? *Communication Research and Practice*, *5*, 105–120. https://doi.org/10.1080/22041451.2019.1601148

Ribeiro, A. (2019, December 20). Semtech uses LoRaWAN network deployment to complement Seoul's citywide Wi-Fi, support plans to grow its smart city IoT environment. *IoT Innovator*. http://iotinnovator.com/semtech-uses-lorawan-network-deployment-to-complement-seouls-citywide-wi-fi-support-plans-to-grow-its-smart-city-iot-environment/

Richardson, M., Bosua, R., Clark, K., Webb, J., Ahmad, A., and Maynard, S. (2016). Privacy and the Internet of Things. *Media and the Arts Law Review*, *21*, 336–351.

Riches, C. (2019, September 2). High-tech bins to tackle Sydney's beach rubbish. *Government News*. https://www.governmentnews.com.au/high-tech-bins-to-tackle-sydneys-beach-rubbish/

Risom, J., Muessig, A., Scharnhorst, E., Jones, T., DeCicco, A., and Dockstader, C. (2016). *The public life diversity toolkit*.

Robertson, A. (2018, September 28). California just became the first state with an Internet of Things cybersecurity law. *The Verge*. https://www.theverge.com/2018/9/28/17874768/california-iot-smart-device-cybersecurity-bill-sb-327-signed-law

Robinson, H., MacDonald, B. A., Kerse, N., and Broadbent, E. (2013). Suitability of Healthcare Robots for a Dementia Unit and Suggested Improvements. *Journal of the American Medical Directors Association*, *14*(1), 34–40. https://doi.org/10.1016/j.jamda.2012.09.006

Robinson, R. (2016, February 1). Why Smart Cities still aren't working for us after 20 years. And how we can fix them. *The Urban Technologist*. https://theurbantechnologist.com/2016/02/01/why-smart-cities-still-arent-working-for-us-after-20-years-and-how-we-can-fix-them/

Roepke, I., Christensen, T., and Jensen, J. (2010). Information and communication technologies - A new round of household electrification. *Energy Policy*, *38*(4), 1764–1773. https://doi.org/10.1016/j.enpol.2009.11.052

Rosin, J. (2018). *Optibus uses artificial intelligence to improve mass transit's on-time performance and prevent delays*.

Royston, S., Selby, J., and Shove, E. (2018). Invisible energy policies: A new agenda for energy demand reduction. *Energy Policy*, *123*, 127–135. https://doi.org/10.1016/j.enpol.2018.08.052

Rural Industries Research & Development Corporation. (2016). *Internet of Things*. https://www.agrifutures.com.au/wp-content/uploads/publications/16-039.pdf

Ryan, T., Allen, K.-A., Gray, D., and McInerney, D. (2017). How Social Are Social Media? A Review of Online Social Behaviour and Connectedness. *Journal of Relationships Research*, *8*. https://doi.org/10.1017/jrr.2017.13

Saad, W., Bennis, M., and Chen, M. (2019). A Vision of 6G Wireless Systems: Applications, Trends, Technologies, and Open Research Problems. *IEEE Network*, *34*(3), 134–142. https://doi.org/10.1109/MNET.001.1900287

Sadowski, J. (2019). When data is capital: datafication, accumulation, and extraction. *Big Data & Society*, *6*(1). https://doi.org/10.1177/2053951718820549

Sadowski, J., and Bendor, R. (2018). Selling Smartness: Corporate Narratives and the Smart City as a Sociotechnical Imaginary. *Science, Technology, & Human Values*, *44*(3), 540–563. https://doi.org/10.1177/0162243918806061

Sadowski, J., Carlson, A., and Osbourne, N. (2020). Darwin's "smart city" project is about surveillance and control. *The Conversation*. https://theconversation.com/darwins-smart-city-project-is-about-surveillance-and-control-127118

Sadowski, J., and Pasquale, F. (2015). The spectrum of control: A social theory of the smart city. *First Monday*, *20*(7). https://doi.org/10.5210/fm.v20i7.5903

Samaras, T., Leitgeb, N., Auvinen, A., Danker-Hopfe, H., Hansson Mild, K., Mattsson, M.-O., Norppa, H., Rubin, G. J., Scarfi, M. R., Schüz, J., Sienkiewicz, Z., and Zeni, O. (2015). *SCENIHR (Scientific Committee on Emerging and Newly Identified Health Risks), Potential health effects of exposure to electromagnetic fields (EMF), 27 January, 2015*. https://doi.org/10.2772/75635

Santofimia, M., Villa, D., Aceña, O., del Toro Garcia, X., Trapero, C., Villanueva, F., and López, J. C. (2018). Enabling smart behavior through automatic service composition for Internet of Things–based Smart Homes. *International Journal of Distributed Sensor Networks*, *14*(8). https://doi.org/10.1177/1550147718794616

Sawyer, M. (2018). *Technology is making cities "smart", but its also costing the environment*. The Conversation. https://theconversation.com/technology-is-making-cities-smart-but-its-also-costing-the-environment-99296

Schmalstieg, D., Langlotz, T., and Billinghurst, M. (2008). Augmented Reality 2.0. In *Virtual Realities: Dagstuhl Seminar 2008*. https://doi.org/10.1007/978-3-211-99178-7_2

Seet, P.-S., and Jones, J. (2019a). Indigenous Art Centres that sustain remote communities are at risk. The VET sector can help. *The Conversation*. http://theconversation.com/indigenous-art-centres-that-sustain-remote-communities-are-at-risk-the-vet-sector-can-help-121179

Seet, P.-S., and Jones, J. (2019b). The government keeps talking about revamping VET – but is it actually doing it? *The Conversation*. https://theconversation.com/the-government-keeps-talking-about-revamping-vet-but-is-it-actually-doing-it-117743

Seet, P.-S., Jones, J., Spoehr, J., and Hordacre, A.-L. (2018). *The Fourth Industrial Revolution: the implications of technological disruption for Australian VET*. NCVER. https://www.ncver.edu.au/research-and-statistics/publications/all-publications/the-fourth-industrial-revolution-the-implications-of-technological-disruption-for-australian-vet

Seet, P.-S., Jones, J., Spoehr, J., and Hordacre, A.-L. (2019, June 25). Jobs are changing, and fast. Here's what the VET sector (and employers) need to do to keep up. *The Conversation*. https://theconversation.com/jobs-are-changing-and-fast-heres-what-the-vet-sector-and-employers-need-to-do-to-keep-up-118524

Sendel, R. (2019). *Your ready-made ecosystem for predictive maintenance*. https://www.ibm.com/blogs/internet-of-things/iot-arrow-electronics/

Sethi, P., and Sarangi, S. R. (2017). Internet of Things: Architectures, Protocols, and Applications. *Journal of Electrical and Computer Engineering*, *2017*, 25.

Sharwood, S. (2020). *It's time to track people's smartphones to ensure they self-isolate during this global pandemic, says WHO boffin*. The Register. theregister.co.uk/2020/03/23/track_phones_coronavirus_who/

Shelton, T., Zook, M., and Wiig, A. (2014). The "actually existing smart city." *Cambridge Journal of Regions, Economy and Society*, *8*, 13–25. https://doi.org/10.1093/cjres/rsu026

Shepherd, T. (2020). Adelaide-based national satellite centre has moved into Lot Fourteen and is looking at futuristic firefighting technology. *The Daily Telegraph*. https://thewest.com.au/news/sa/adelaide-based-national-satellite-centre-has-moved-into-lot-fourteen-and-is-looking-at-futuristic-firefighting-technology-ng-d6453799b0bf79233872f09238e80c38

Shieber, J. (2019). *The Los Angeles Fire Department wants more drones*. Tech Crunch. https://techcrunch.com/2019/10/20/the-los-angeles-fire-department-wants-more-drones/

Shove, E. (2003). *Comfort, Cleanliness and Convenience: The Social Organisation of Normality*. Berg Publishers.

Shove, E., and Walker, G. (2014). What Is Energy For? Social Practice and Energy Demand. *Theory, Culture & Society*, *31*, 41–58. https://doi.org/10.1177/0263276414536746

Sinha, R. S., Wei, Y., and Hwang, S.-H. (2017). A survey on LPWA technology: LoRa and NB-IoT. *ICT Express*, *3*(1), 14–21. https://doi.org/https://doi.org/10.1016/j.icte.2017.03.004

Smith, N., Bardzell, S., and Bardzell, J. (2017). Designing for Cohabitation: Naturecultures, Hybrids, and Decentering the Human in Design. *CHI '17: Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 1714–1725. https://doi.org/10.1145/3025453.3025948

Spieser, K., Treleaven, K., Zhang, R., Frazzoli, E., Morton, D., and Pavone, M. (2014). *Toward a Systematic Approach to the Design and Evaluation of Automated Mobility-on-Demand Systems: A Case Study in Singapore*. 0–16.

Stanford. (2019). *Internet of Things Graduate Certificate*. https://online.stanford.edu/programs/internet-things-graduate-certificate

Strava. (2019). *The Global Heatmap*. https://www.strava.com/heatmap#7.00/-120.90000/38.36000/hot/all

Strengers, Y. (2013). *Smart Energy Technologies in Everyday Life: Smart Utopia?* Palgrave Macmillan UK. https://doi.org/10.1057/9781137267054

Strengers, Y., Kennedy, J., Arcari, P., Nicholls, L., and Gregg, M. (2019). Protection, Productivity and Pleasure in the Smart Home. *CHI '19 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems: Weaving The Threads Of CHI*.

Strengers, Y., and Nicholls, L. (2017). Convenience and energy consumption in the smart home of the future: Industry visions from Australia and beyond. *Energy Research & Social Science*, *32*. https://doi.org/10.1016/j.erss.2017.02.008

Strengers, Y., Nicholls, L., Glover, A., Arcari, P., and Martin, R. (2019). *Engaging Households Towards the Future Grid: An Engagement Strategy for the Energy Sector*. https://www.monash.edu/__data/assets/pdf_file/0004/1862833/Engaging-households-towards-the-Future-Grid-FINAL-181219.pdf

Strengers, Y., Pink, S., and Nicholls, L. (2019). Smart energy futures and social practice imaginaries: Forecasting scenarios for pet care in Australian homes. *Energy Research & Social Science*, *48*, 108–115. https://doi.org/10.1016/j.erss.2018.09.015

Sundaravadivel, P., Kougianos, E., Mohanty, S., and Ganapathiraju, M. (2018). Everything You Wanted to Know about Smart Health Care: Evaluating the Different Technologies and Components of the Internet of Things for Better Health. *IEEE Consumer Electronics Magazine*, *7*, 18–28. https://doi.org/10.1109/MCE.2017.2755378

Suseno, Y., and Standing, C. (2018). The Systems Perspective of National Innovation Ecosystems. *Systems Research and Behavioral Science*, *35*(3), 282–307. https://doi.org/10.1002/sres.2494

Swan, M. (2012). Sensor Mania! The Internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2.0. *Journal of Sensor and Actuator Networks*, *1*, 217–253. https://doi.org/10.3390/jsan1030217

Tahiliani, V., and Dizalwar, M. (2018). Green IoT systems: An energy efficient perspective. *2018 Eleventh International Conference on Contemporary Computing (IC3)*, 1–6.

Tanczer, L., Brass, I., Elsden, M., Carr, M., and Blackstock, J. J. (2019). The United Kingdom's Emerging Internet of Things (IoT) Policy Landscape. In R. Ellis & V. Mohan (Eds.), *Rewired: Cybersecurity Governance* (pp. 37–56). Wiley.

Tashjian, V., Mosadeghi, S., Howard, A., Lopez, M., Dupuy, T., Reid, M., Martinez, B., Ahmed, S., Dailey, F., Robbins, K., Rosen, B., Fuller, G., Danovitch, I., IsHak FAPA, Waguih, M. D., and Spiegel, B. (2017). Virtual Reality for Management of Pain in Hospitalized Patients: Results of a Controlled Trial. *JMIR Mental Health*, *4*, e9. https://doi.org/10.2196/mental.7387

Taylor Buck, N., and While, A. (2015). Competitive urbanism and the limits to smart city innovation: The UK Future Cities initiative. *Urban Studies*, *54*. https://doi.org/10.1177/0042098015597162

Tchetvertakov, G. (2020). *Beam Communications launches satellite-powered messaging solution Zoleo*. Small Caps. https://smallcaps.com.au/beam-communications-launches-satellite-powered-messaging-solution-zoleo/

Telstra, and Penn, A. (2020). *Half year 2020 results*. https://www.telstra.com.au/content/dam/tcom/about-us/investors/pdf F/130220-1H20-Analyst-Presentation.pdf

Telsyte. (2019). *Australian IoT@Home Market Cracks $1BN, Paving the way for IoT-Commerce Services*. https://www.telsyte.com.au/announcements/2019/5/14/australian-iothome-market-cracks-1bn-paving-the-way-for-iot-commerce-services

The Climate Council. (2016). *On the Frontline: Climate Change & Rural Communities*. https://www.climatecouncil.org.au/uploads/564abfd96ebac5cbc6cf45de2f17e12d.pdf

The Government of Japan. (2015). *Cybersecurity Strategy*. https://www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf

Thomas, J., Barraket, J., Wilson, C., Rennie, E., Ewing, S., and MacDonald, T. (2019). *Measuring Australia's Digital Divide: The Australian Digital Inclusion Index 2019*. https://digitalinclusionindex.org.au/wp-content/uploads/2019/10/TLS_ADII_Report-2019_Final_web_.pdf

Ting, D. S. W., Carin, L., Dzau, V., and Wong, T. Y. (2020). Digital technology and COVID-19. *Nature Medicine*, *26*(4), 459–461. https://doi.org/10.1038/s41591-020-0824-5

Transmax. (2018). *Case Study: Streams Smart Motorways*. https://www.transmax.com.au/wp-content/uploads/2018/01/Case-Study_Smart-Motorways-.pdf

Transport NSW. (2020). *On Demand Public Transport*. https://transportnsw.info/travel-info/ways-to-get-around/on-demand

Tsui, M. (2013). The state of the art defence: defining the Australian experience in the context of pharmaceuticals. *QUT L. Rev.*, *13*, 132.

Tuffley, D. (2019). *Virtual tools, real fires: how holograms and other tech could help outsmart bushfires*. The Conversation. https://theconversation.com/virtual-tools-real-fires-how-holograms-and-other-tech-could-help-outsmart-bushfires-126830

Turcu, C. O., and Elena, C. (2018). Industrial Internet of Things as a Challenge for Higher Education. *International Journal of Advanced Computer Science and Applications*, *9*(11), 55–60. https://doi.org/10.14569/IJACSA.2018.091108

Article 23(1), Universal Declaration of Human Rights, (1948).

Unify-IoT. (2016). *Deliverable D03.01 Report on IoT platform activities*. http://www.internet-of-things-research.eu/pdf/D03_01_WP03_H2020_UNIFY-IoT_Final.pdf

Universidad Carlos III de Madrid. (2019). *Drones for early detection of forest fires*. https://www.uc3m.es/ss/Satellite/UC3MInstitucional/en/Detalle/Comunicacion_C/1371271588512/1371216052710/Drones_for_early_detection_of_forest_fires

University of New England. (2020). *UNE's COVID-19 Virtual Care Response pilot monitors arrive*.

University of South Australia. (2020). *UniSA working on "pandemic drone" to detect coronavirus*.

University of Technology Sydney. (2019). *Prepare your IoT future masterclass*. https://open.uts.edu.au/uts-open/faculty/engineering-and-information-technology/internet-of-things/

UNSGSA FinTech Working Group and CCAF. (2019). *Early Lessons on Regulatory Innovations to Enable Inclusive FinTech: Innovation Offices, Regulatory Sandboxes, and RegTech*. https://www.unsgsa.org/files/3515/5007/5518/UNSGSA_Report_2019_Final-compressed.pdf

US Department of Energy. (2019). *Recovery Act: Smart Grid Workforce Training and Development*. SmartGrid.Gov. https://www.smartgrid.gov/recovery_act/overview/workforce_training.html

van der Graaf, S., and Ballon, P. (2019). Navigating Platform Urbanism. *Technological Forecasting and Social Change*, *142*, 364–372. https://doi.org/10.1016/j.techfore.2018.07.027

van Dijck, J., Poell, T., and de Waal, M. (2018). *The Platform Society: Public Values in a Connective Society*. Oxford University Press.

van Eck, N. J., and Waltman, L. (2010). Software survey: VOSviewer, a computer program for bibliometric mapping. *Scientometrics*, *84*, 523–538. https://doi.org/10.1007/s11192-009-0146-3

van Eck, N. J., and Waltman, L. (2014). Visualizing Bibliometric Networks. In Y. Ding, R. Rousseau, & D. Wolfram (Eds.), *Measuring Scholarly Impact: Methods and Practice*. Springer International Publishing.

Vanolo, A. (2016). Is there anybody out there? The place and role of citizens in tomorrow's smart cities. *Futures*, *82*. https://doi.org/10.1016/j.futures.2016.05.010

Varona, B., Monteserin, A., and Teyseyre, A. (2019). A deep learning approach to automatic road surface monitoring and pothole detection. *Personal and Ubiquitous Computing*. https://doi.org/10.1007/s00779-019-01234-z

Vega-Barbas, M., Casado-Mansilla, D., Valero, M. A., Lopez-de-Ipina, D., Bravo, J., and Florez, F. (2012). Smart Spaces and Smart Objects Interoperability Architecture (S3OiA). *Proceedings of the 2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, 725–730. https://doi.org/10.1109/IMIS.2012.99

Vi Dimensions. (2019). *The future of smart surveillance*. https://vidimensions.com

Victorian Government. (2018). *A Data Reform Strategy for the Victorian Public Service: Better decisions underpinned by data.* https://www.vic.gov.au/sites/default/files/2019-02/A-Data-Reform-Strategy-for-the-VPS.pdf

Vodafone. (2019). *A new IoT regulatory framework for Europe*. https://www.vodafone.com/content/dam/vodcom/files/public-policy/iot-whitepaper/IoT_whitepaper_.pdf

Voutsinos, M. (2018). *Biomining the elements of the future*. The Conversation. https://theconversation.com/biomining-the-elements-of-the-future-87621

Waldman, P., and Mulvany, L. (2020). *Farmers Fight John Deere Over Who Gets to Fix an $800,000 Tractor*. Bloomberg News. https://www.bloomberg.com/news/features/2020-03-05/farmers-fight-john-deere-over-who-gets-to-fix-an-800-000-tractor

Walsh, M., and Pan, N. (2018). What's next for Chinese tech giant Huawei after being banned from Australia's 5G network? *ABC News*. https://www.abc.net.au/news/2018-08-25/whats-next-for-huawei-after-being-banned-from-australias-5g/10160842

Walsh, T., Levy, N., Bell, G., Elliott, A., Mareels, I. M. Y., and Wood, F. (2019). *The Effective and Ethical Development of Artificial Intelligence: An opportunity to improve our wellbeing Report for the Australian Council of Learned Academies*. https://acola.org/hs4-artificial-intelligence-australia/

Wang, S. J., and Moriarty, P. (2019). Energy savings from Smart Cities: A critical analysis. *Energy Procedia*, *158*, 3271–3276. https://doi.org/10.1016/j.egypro.2019.01.985

We Ride Australia. (2018). *The power of an image! The Canberra Transport Photo.* https://www.weride.org.au/events/the-power-of-an-image-the-canberra-transport-photo/

Weiss, A. (2019). GAIA-X: Growing a vibrant European ecosystem. *Dot Magazine*. https://www.dotmagazine.online/issues/on-the-edge-building-the-foundations-for-the-future/gaia-x-a-vibrant-european-ecosystem

West, M., Kraut, R., and Chew, H. . (2019). *I'd blush if I could: Closing Gender Divides in Digital Skills Through Education*. https://en.unesco.org/Id-blush-if-I-could

Western Power. (2019). *SPS is empowering regional communities*. https://westernpower.com.au/our-energy-evolution/grid-technology/stand-alone-power-system

Westwood, T., Gupta, M., and Hughes, N. (2019). *Water markets outlook: August 2019, ABARES research report 19.9*. https://www.agriculture.gov.au/sites/default/files/abares/documents/WaterMarketOutlook_August2019_v1.0.0.pdf

Whitehead, B., Andrews, D., Shah, A., and Maidment, G. (2014). Assessing the environmental impact of data centres part 1: Background, energy use and metrics. *Building and Environment*, *82*, 151–159. https://doi.org/https://doi.org/10.1016/j.buildenv.2014.08.021

Whittaker, Z. (2019). *Security flaws in a popular smart home hub let hackers unlock front doors*. Tech Crunch. https://techcrunch.com/2019/07/02/smart-home-hub-flaws-unlock-doors/

Wilsmore, B., and Leitch, J. (2017). Remote monitoring of medical devices in Australia. *The Medical Journal of Australia*, *206*(2), 62–63. https://doi.org/10.5694/mja16.00730

Wilson, K. (2019). *Mending hearts: how a "repair economy" creates a kinder, more caring community*. The Conversation. https://theconversation.com/mending-hearts-how-a-repair-economy-creates-a-kinder-more-caring-community-113547

Winter, S. J. (2019). Who Benefits? *Communications of the ACM*, *62*(7), 23–25. https://doi.org/10.1145/3332807

Winther, T., Ulsrud, K., Matinga, M., Govindan, M., Gill, B., Saini, A., Brahmachari, D., Palit, D., and Murali, R. (2019). In the light of what we cannot see: Exploring the interconnections between gender and electricity access. *Energy Research & Social Science*, *60*. https://doi.org/10.1016/j.erss.2019.101334

World Economic Forum. (2016). *The Future of Jobs: Employment, Skills and Workforce Strategy for the Fourth Industrial Revolution*. http://www3.weforum.org/docs/WEF_Future_of_Jobs.pdf

World Manufacturing Foundation. (2019). *2019 World Manufacturing Forum Report, Skills for the Future of Manufacturing*. https://c00e521c-fc35-464f-8eef-9356e02fbfb5.filesusr.com/ugd/c56fe3_d617f7333fd347b0b2bb4a739ba72993.pdf

Wray, S. (2018). *Copenhagen shares takeaways from its City Data Exchange*. SmartCitiesWorld2. https://www.smartcitiesworld.net/news/news/copenhagen-shares-takeaways-from-its-city-data-exchange-2961

WSP. (2018). *Design for a better future - Infrastructure Victoria: ICT Infrastructure Advice for Automated and Zero Emission Vehicles*. https://www.infrastructurevictoria.com.au/wp-content/uploads/2019/04/ICT_Infrastructure_Advice_for_Automated_and_Zero_Emission_Vehicles.pdf

Xu, X., Zeng, Z., Wang, Y., and Ash, J. (2019). A Framework of a V2X Communication System for Enhancing Vehicle and Pedestrian Safety at Un-Signalized Intersections. In J. Xu, F. Cooke, M. Gen, & S. Ahmed (Eds.), *Proceedings of the Twelfth International Conference on Management Science and Engineering Management. ICMSEM 2018.* (pp. 51–63). Springer Cham. https://doi.org/https://doi.org/10.1007/978-3-319-93351-1_5

Yigitcanlar, T., Foth, M., and Kamruzzaman, M. (2019). Towards Post-Anthropocentric Cities: Reconceptualizing Smart Cities to Evade Urban Ecocide. *Journal of Urban Technology*, *26*(2), 147–152. https://doi.org/https://doi.org/10.1080/10630732.2018.1524249

Yigitcanlar, T., Hewa, H. K., Ruth, N. E., Butler, L., Vella, K., and Desouza, K. (2020). *Smart Cities Down Under: Performance of Australian Local Government Areas*. Queensland University of Technology. https://eprints.qut.edu.au/136873/

Yoshida, J. (2019). *The DSRC vs 5G Debate Continues*. EET Asia. https://www.eetasia.com/news/article/The-DSRC-vs-5G-Debate-Continues

Yu, A., Lo, A., Clarke, R., Farbenblum, B., Joyce, D., Leeuw, M. De, Bennett Moses, L., Manwaring, K., Nolan, J., and Zalnieriute, M. (2019). *Response to Issues Paper on Human Rights and Technology*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3346196

Yu, W., and Xu, C. (2018). Developing Smart Cities in China: An Empirical Analysis. *International Journal of Public Administration in the Digital Age (IJPADA)*, *5*(3), 76–91. https://doi.org/10.4018/IJPADA.2018070106

Yuvaraj, J. (2018). How about me? The scope of personal information under the Australian Privacy Act 1988. *Computer Law & Security Review*, *34*(1), 47–66. https://doi.org/10.1016/j.clsr.2017.05.019

Zallio, M., and Berry, D. (2017). Design and Planned Obsolescence. Theories and Approaches for Designing Enabling Technologies. *The Design Journal*, *20*, S3749–S3761. https://doi.org/10.1080/14606925.2017.1352879

Zetter, K. (2015). *Medical Devices That Are Vulnerable to Life-Threatening Hacks*. Wired. https://www.wired.com/2015/11/medical-devices-that-are-vulnerable-to-life-threatening-hacks/#slide-x

Zhang, A., Jakku, E., Llewellyn, R., and Baker, E. I. (2018). Surveying the needs and drivers for digital agriculture in Australia. *Farm Policy Journal*, *15*(1), 25–37.

Zhang, L., Li, J.-Q., Zhou, K., Gupta, S., Li, M., Zhang, W.-B., Miller, M., and Misener, J. (2011). Traveler Information Tool with Integrated Real-Time Transit Information and Multimodal Trip Planning. *Transportation Research Record: Journal of the Transportation Research Board*, *2215*, 1–10. https://doi.org/10.3141/2215-01

Zhong, R. Y., Xu, X., Klotz, E., and Newman, S. T. (2017). Intelligent manufacturing in the context of industry 4.0: a review. *Engineering*, *3*(5), 616–630.

Zografos, K., Spitadakis, V., and Androutsopoulos, K. (2008). Integrated Passenger Information System for Multimodal Trip Planning. *Transportation Research Record: Journal of the Transportation Research Board*, *2072*(1), 20–29. https://doi.org/10.3141/2072-03

Zoonen, L. (2016). Privacy concerns in smart cities. *Government Information Quarterly*, *33*, 472–480. https://doi.org/10.1016/j.giq.2016.06.004

EXPERT WORKING GROUP

Professor Bronwyn Fox FTSE (Chair)

Professor Bronwyn Fox is the Deputy Vice Chancellor, Research and Enterprise, at Swinburne University of Technology. She has been instrumental in positioning Swinburne at the forefront of manufacturing, building extensively on Swinburne's Industry 4.0 initiatives and capabilities. She has led a number of significant initiatives and research partnerships through her role as the founding Director of Swinburne's Manufacturing Futures Research Institute, including:

- establishing the world's first Industry 4.0 Testlab for additive manufacturing of carbon fibre composites in partnership with the CSIRO
- collaborating with ARENA2036, a flexible factory of the future on the University of Stuttgart's Baden-Wüerttemberg campus
- leading the development, innovation and commercialisation of graphene applications, as part of the Graphene Supply Chain CRC-P.

She has demonstrated a sustained commitment to support the growth of the carbon fibre and composite industry in Australia through targeted research and was previously a co-founder of the Carbon Nexus facility at Deakin University, a core part of a $100 million precinct in Geelong. Professor Fox is the Chair of the Australian Academy of Technology and Engineering Victorian Division. She is a Fellow of the Academy of Technology and Engineering, a Fellow of the Royal Australian Chemical Institute and a Graduate of the Australian Institute of Company Directors. In 2018, Professor Fox was awarded the GCMM Research Leadership Award at the 14th Global Congress on Manufacturing and Management.

Professor Gerard Goggin FAHA

Gerard Goggin is Wee Kim Wee Professor of Communication Studies at Nanyang Technological University, Singapore. He is also Professor of Media and Communications at the University of Sydney. Professor Goggin's work focuses on the social, cultural and political dynamics of emerging technologies, such as mobile communication and media, apps, and the IoT. He has had a long-standing involvement in consumer, citizen and social justice issues in digital technology and was a founding board member of the Australian Communications Consumer Action Network. Key publications include *Location Technologies in International Context* (2020), *Routledge Companion to Disability and Media* (2020), *Routledge Companion to Global Internet Histories* (2017), *Global Mobile Media* (2011), *Cell Phone Culture* (2006), *Disability in Australia* (2005), *Virtual Nation: The Internet in Australia* (2004), and *Digital Disability* (2003). Professor Goggin is a Fellow of the Australian Academy of Humanities, and also the International Communication Association. Among other roles, he served as Chair of the Humanities and Creative Arts Panel of the ARC's inaugural Engagement and Impact Assessment.

Professor Deborah Lupton FASSA

Deborah Lupton is SHARP Professor in the Faculty of Arts & Social Sciences, UNSW Sydney, working in the Centre for Social Research in Health; the Social Policy Research Centre; and leading the Vitalities Lab. She is the author and co-author of 17 books, the latest of which are *Digital Sociology* (Routledge, 2015), *The Quantified Self* (Polity, 2016), *Digital Health* (Routledge, 2017), *Fat, 2nd edition* (Routledge, 2018) and *Data*

Selves (Polity, 2019). Professor Lupton is a Chief Investigator and leader of the UNSW Node of the Australian Research Council Centre of Excellence in Automated Decision-Making and Society (2020–2026). She is currently serving as a Commissioner on The Lancet and Financial Times Commission 'Governing Health Futures 2030: Growing Up in a Digital World' (2019–2021). She is a Fellow of the Academy of the Social Sciences in Australia and holds an Honorary Doctor of Social Science degree awarded by the University of Copenhagen.

Professor Holger Regenbrecht (New Zealand Royal Society Te Apārangi)

Holger Regenbrecht is a computer scientist and Professor in the Department of Information Science at the University of Otago, New Zealand. His work spans theory, concepts, techniques, technologies and applications. Holger's research interests include human–computer interaction, applied computer science and information technology, presence and telepresence, ubiquitous, immersive and collaborative augmented reality, three-dimensional user interfaces, psychological aspects of virtual and mixed reality, computer-aided therapy, VR learning and collaboration.

He has published over 100 peer-reviewed articles and has over 5000 citations to his work. His current work focuses on translational research and on understanding and implementing computer-mediated realities.

He is a member of several international professional groups and serves as an editorial board member, reviewer and auditor for a number of conferences, journals and institutions. Holger is the current Head of the Information Science department.

Professor Paul Scuffham FAHMS

Paul Scuffham is a Professor of Health Economics at Griffith University, Gold Coast, Australia, and a NHMRC Senior Research Fellow. His research interests are focused on modelling the costs and benefits of health care interventions, measurement and valuation of health outcomes, priority setting, and evaluating methods for formally incorporating the public in health policy decision making. His research places an emphasis on the translation of research into health policy.

He is the Director of the Menzies Health Institute Queensland and former Director of the Centre for Applied Health Economics at Griffith University. He was the founding President of the Australian Chapter of the International Society for Pharmacoeconomics and Outcomes Research (ISPOR-AC), Graduate of the Australian Institute of Company Directors, and is a Fellow and Council member of the Australian Academy of Health and Medical Science.

Professor Branka Vucetic FAA FTSE

Branka Vucetic is an ARC Laureate and Director of the Centre for IoT and Telecommunications at the University of Sydney.

Her current research work is in wireless networks and the IoT. In the area of wireless networks, she works on communication system design for millimetre wave frequency bands. In the area of the IoT, Vucetic works on providing wireless connectivity for mission critical applications.

Branka Vucetic is a Fellow of the IEEE, the Australian Academy of Technological Sciences and Engineering and the Australian Academy of Science.

PEER REVIEW PANEL

This report has been reviewed by an independent panel of experts. Members of this review panel were not asked to endorse the report's conclusions and findings. The Review Panel members acted in a personal, not organisational, capacity and were asked to declare any conflicts of interest. ACOLA gratefully acknowledges their contribution.

Professor Dacheng Tao FAA

Professor Dacheng Tao is an Australian Laureate Fellow, Professor of Computer Science and the Inaugural Director of the UBTECH Sydney Artificial Intelligence Centre at The University of Sydney. His research results in AI have been expounded in one monograph and more than 300 publications in leading journals and conferences, with many best paper awards, such as the 2014 ICDM 10-year highest-impact paper award, the 2017 IEEE Signal Processing Society Best Paper Award, and the 2018 IJCAI distinguished paper award. His publications have received over 51,000 citations. He is a highly cited researcher in both engineering (since 2014) and computer science (since 2015) and has an h-index 117. He received the 2015 Australian Scopus-Eureka Prize and the 2018 IEEE ICDM Research Contributions Award. He is a Fellow of the Australian Academy of Science, a Foreign Member of the Academia Europaea and a Fellow of the American Association for the Advancement of Science, Association for Computing Machinery, IEEE, and Optical Society of America.

Professor Julian Thomas FAHA

Julian Thomas is Director of the ARC Centre of Excellence for Automated Decision-making and Society, and a Professor in the School of Media and Communications at RMIT University. He leads the team producing the Australian Digital Inclusion Index (Telstra, 2016) and publishes widely on the social aspects of new communications technologies. Thomas' books include *Internet on the Outstation: The Digital Divide and Remote Aboriginal Communities* (INC, 2016), and *The Informal Media Economy* (Polity, 2015). He is a Fellow and council member of the Australian Academy of the Humanities.

Dr Jathan Sadowski

Jathan Sadowski is a research fellow in the Emerging Technologies Research Lab in the Faculty of Information Technology at Monash University. His work focuses on the political economy of technology by asking critical questions that seek to analyse the interests, imperatives and ideologies that influence the design and use of technical systems. He has done extensive work on topics such as smart cities, data collection and digital platforms. Jathan is the author of *Too Smart: How Digital Capitalism is Extracting Data, Controlling Our Lives, and Taking Over the World* (The MIT Press).

Professor Glenn Wightwick FTSE

Professor Glenn Wightwick is the Deputy Vice-Chancellor of Innovation and Enterprise at the University of Technology Sydney (UTS), where he has responsibility for the university's innovation, entrepreneurship and industry engagement. Prior to this he was Deputy Vice-Chancellor of Research for three and a half years. He spent 27 years working at IBM in Australia, the US and China in a variety of technical and leadership roles in systems engineering, development and research. He is a Fellow of the Australian Academy of Technology and Engineering and a Senior Fellow of the Institute of Electrical and Electronic Engineers. He is Co-Chair of 2SER, a community radio station jointly owned by UTS and Macquarie University and is on the board of the Sydney School of Entrepreneurship.

ACKNOWLEDGEMENTS

ACOLA and the Expert Working Group offer their sincere gratitude to the many experts across Australia who have contributed to the evidence gathering of this report. In particular, we would like to acknowledge the expert contributors, research organisations, peak groups, government bodies and industry organisations who took the time to contribute to the project by way of input papers, submissions and consultation sessions. Further information on these contributions can be found in 'Evidence gathering'.

We also gratefully acknowledge the expertise and contributions from our project stakeholders, and their ongoing support throughout the development of this report. In particular, we would like to acknowledge Dr Alan Finkel, Dr Penny Leggett, and Emma Wisdom, from the Office of the Chief Scientist; Luisa Powell and Liz Visher from the Australian Research Council; and Sally Todd, Stephen Briggs, Philip Mason, Dr Jason Ashurst, Alice McRorie, Isabelle Cox, Dr Alexander Pound, Alex Wilson and Georgianna Duggan, from the Department of Infrastructure, Transport, Regional Development and Communications.

We also thank our peer reviewers for their valuable contributions in reviewing the report.

We would particularly like to thank the Australian Research Council (project number CS170100007) and the Department of Infrastructure, Transport, Regional Development and Communications for their financial support and contributions to the project.

Our sincere thanks and gratitude to the Expert Working Group, who put a great deal of time, effort and strategic insight into coordinating the report's conceptualisation and production, and also to the ACOLA team, in particular Stephanie Chan, Ella Relf, Dr Lauren Palmer and Ryan Winn who made significant contributions to supporting the Expert Working Group and managing the project.

EVIDENCE GATHERING

Many people have contributed their time and expertise to the project through written submissions, meetings with members of the Expert Working Group and participating in consultations. Consultations and meetings were held across Australia and internationally during this project. The development of the report has been made possible through their generous contributions.

In particular, we would like to thank Kayleen Manwaring, Hussein Dia and Jason Potts for their significant contributions to the development of this report.

The views expressed in this report do not necessarily reflect the opinions of the people and organisations listed in the following sections.

Written submissions

As part of the evidence gathering to support the development of the report, a call for input was sent to experts in the field. ACOLA and the Expert Working Group would like to sincerely thank the following organisations and people.

Advanced manufacturing
Bronwyn Fox

Cybersecurity
Vijay Varadharajan

Economic analysis
Jason Potts

Energy consumption and novel social experiences of IoT
Yolande Strengers, Larissa Nicholls, Sarah Pink

Energy implications of the IoT
Rod Tucker

Freight and logistics
Kim Hassall

Healthcare and health service delivery
Jaimon T. Kelly, Katrina L. Campbell, Paul Scuffham

IoT and the future workplace
Pi-Shen Seet, Janice Jones, Anton Klarin, Yuliani Suseno

IoT and indigenous communities
Tyson Yunkaporta

Legal, ethical and human rights
Kayleen Manwaring
Herbert Smith Freehills – Tony Joyner, Natasha Blycha, Alex Cook with support from Ariane Garside, Michael Faithfull, Oli Tod, Rafael Lawrence

Novel data and information considerations with IoT
David Eyers, Holger Regenbrecht

Monitoring and surveillance in the contemporary workplace
Peter Holland

Psychological impacts of IoT
Kit Huckvale

Radiation and 5G
Australian Radiation Protection and Nuclear Safety Agency (ARPANSA)

Satellite and space technology
Australian Space Agency – Megan Clark

Service delivery, philanthropy and creative sectors
Sarah Barns
Josh Reid Jones

Smart homes and cities
Internet of Things Alliance Australia – Geoff Heydon, Frank Zeichner

Smart mobility
Hussein Dia, Rusul Abduljabbar, Sohani Liyanage

Sustainability and environmental impact
Marcus Foth, Peta Mitchell, Monique Mann, Markus Rittenbruch, Irina Anastasiu

Social considerations
Deborah Lupton

Telecommunications
Zhanwei Hou with contributions from Peng Cheng, Wibowo Hardjawana, Yifan Gu, Branka Vucetic

Ubiquitous interfaces and pervasive augmented reality
Tobias Langlotz, Holger Regenbrecht

Stakeholder consultation

ACOLA and the Expert Working Group also thank the following stakeholders for their generous time and participation in consultations and contributions to the development of this report.

3A Institute

ACT Government
Chief Digital Officer

Attorney-General's Department

Australian Communications and Media Authority

Australian Communications Consumer Action Network

Australian Cyber Security Centre

Australian Digital Health Agency

Australian Mobile Telecommunications Association

Austroads

Bosch Australia

Bureau of Communications and the Arts Research

CHOICE (Australian Consumers' Association)

Data 61, CSIRO

David Hyland-Wood

Department of Education, Skills and Employment

Department of Industry, Science, Energy and Resources

Department of the Prime Minister and Cabinet

Dominik Rohrmus

Hugh Bradlow

Hussein Dia

IBM Research – Australia

Infrastructure Victoria

ITS Australia

Internet of Things Alliance Australia

NT Government

Office of the National Data Commissioner

Paul Brooks

Pi-Shen Seet

Standards Australia

Volkmar Dietrich

Western Australia Department of Transport

Western Australian Local Government Association

HORIZON SCANNING

ACOLA™

AUSTRALIAN COUNCIL OF LEARNED ACADEMIES