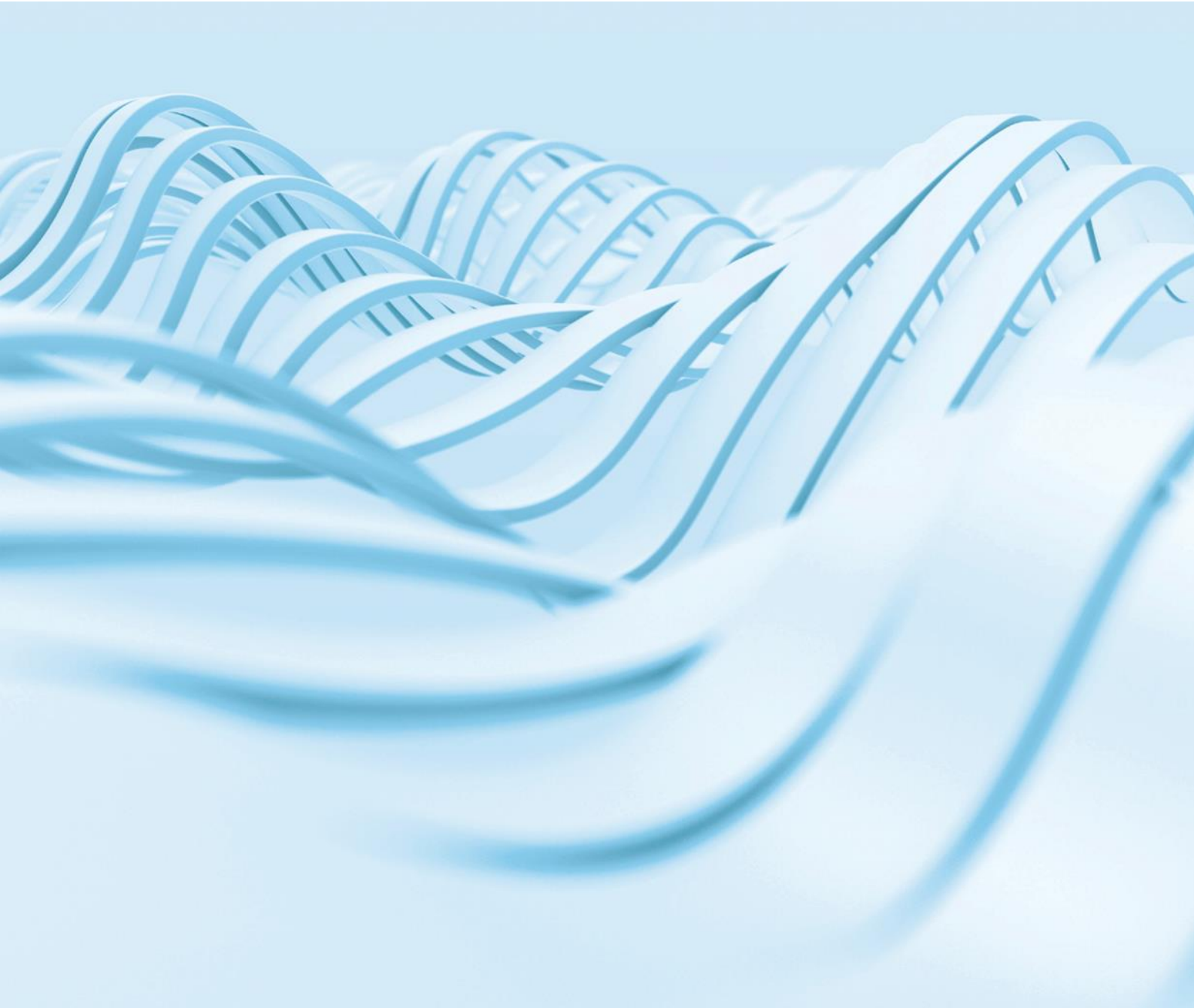
Australian Government
Productivity Commission

Report no. 100 – 7 February 2023

5-year Productivity Inquiry: Australia's data and digital dividend

Inquiry report – *volume 4*



The Productivity Commission acknowledges the Traditional Owners of Country throughout Australia and their continuing connection to land, waters and community. We pay our respects to their Cultures, Country and Elders past and present.

The Productivity Commission

The Productivity Commission is the Australian Government's independent research and advisory body on a range of economic, social and environmental issues affecting the welfare of Australians. Its role, expressed most simply, is to help governments make better policies, in the long term interest of the Australian community.

The Commission's independence is underpinned by an Act of Parliament. Its processes and outputs are open to public scrutiny and are driven by concern for the wellbeing of the community as a whole.

Further information on the Productivity Commission can be obtained from the Commission's website (www.pc.gov.au).

ISSN 1447-1337 (online)
ISSN 1447-1329 (print)
ISBN 978-1-74037-759-1 (set)
ISBN 978-1-74037-763-8 (volume 4)

An appropriate reference for this publication is:
Productivity Commission 2023, *5-year Productivity Inquiry: Australia's data and digital dividend*, Vol. 4, Inquiry Report no. 100, Canberra

Publication enquiries:
Media, Publications and Web | phone 03 9653 2244 | email publications@pc.gov.au

Contents

The Commission's report is divided into 9 volumes: an overview document (volume 1) that presents our policy agenda, and inquiry content volumes (volumes 2–9) that explain in greater detail the reforms that make up the policy agenda, including a modelling appendix. The full report is available from www.pc.gov.au.

Preface

Digital technology and data have transformed our economy and society. In just a couple of decades, smartphones have become ubiquitous, social media has changed the way we communicate and consume content and the volume of data we produce has increased exponentially. These trends have accelerated following the COVID-19 pandemic — e-commerce via online retail purchases, online delivery of human services and digitally enabled work from home are now widespread across Australia.

The **benefits for productivity of increasing digitisation are diverse and diffuse**. In many cases, they arise from technology enabling us to collect, transmit and analyse data more cheaply and quickly than ever before. Consumers can now easily search for products that best meet their preferences and verify product quality through online information. Businesses can deliver services more flexibly and efficiently as technology and data enable faster adjustments, increased scale at lower cost and innovation opportunities. And governments can make better-informed decisions about policy design and implementation, both at the system level and to address local community needs.

Crucially, **many of these benefits are particularly evident in services sectors**, which have historically had more difficulty achieving productivity growth. The positive impacts of digitisation and data use can also extend beyond productivity, by improving economic and social inclusion and living standards more broadly.

Australians are already adopting digital and data tools as they recognise the potential gains. Almost all businesses are connected to the internet, over half have a web presence, 68% have placed orders over the internet and 57% have adopted cloud technology. Growing adoption often follows from businesses' (and individuals') private assessments that the benefits of technology and data use exceed the costs, with little government support required.

Nonetheless, Australia's digital and data transformation is far from complete. Technology changes rapidly and **new productivity-enhancing applications are continuously emerging**.

Technologies such as artificial intelligence (AI), the internet of things (IoT), robotic automation and big data analytics could revolutionise how businesses operate across the economy — and, indeed, are already disrupting various sectors. The productivity gains can be significant, from robot-assisted warehouses that automate online order fulfilment and reduce accidents, to AI-enabled IoT sensors installed in smart cities that allow real-time optimisation of infrastructure, energy and service use and maintenance notification.

Many of these emerging digital and data applications do not merely lead to cost reductions, but can also result in better-quality goods and services and more product choice for consumers. Australia needs to **keep pace with technological developments** to underpin our future economic prosperity.

However, several factors could limit further adoption among Australian businesses — **inadequate internet, lack of skills, low awareness and uncertainty about benefits, security concerns, cost and legacy systems** are identified as barriers. And while we do well compared with other developed economies on foundational aspects of technology and data use (such as internet connections and data volumes), we are falling behind on some more advanced indicators. Australia's internet speeds are relatively low and business use of data-driven technologies, such as AI and analytics, trails uptake in other countries.

Some of these issues will be resolved with further technological progress, as has occurred with previous changes. Emerging applications of technology will become more widely known, and growing awareness of

their uses and benefits will facilitate more uptake as adoption shifts from the small share of early innovators to the mainstream majority of businesses (moving up the technology adoption 'S curve'). The costs of implementing new digital and data solutions are also likely to decrease over time, as computing power continues to improve and economies of scale increase with adoption, and as basic digital skills in the population are improved with each successive generation.

But in other instances, **government can play a role in facilitating more and better use of technology and data**. This is particularly the case when government agencies provide, regulate or fund a service, or when the factors limiting uptake are systemwide issues that can be addressed through broader policy enablers, such as incentive frameworks or access rights. In this volume, the Commission identifies three such enablers where government investments and policies provide foundations for adopting productivity-enhancing digital and data tools, and suggests potential improvements.

- **Digital infrastructure, particularly in regional and remote Australia**, is required to deliver productivity-enhancing access to low-cost and reliable internet for local businesses and workers, and increases social inclusion by ensuring that regional and remote Australians can access quality essential services and expertise that are increasingly available online. Government already invests in regional digital infrastructure, but current funding often lacks transparency and accountability. Transitioning to a technology-neutral tender mechanism for allocating funding when market conditions allow could increase efficiency and transparency while guaranteeing minimum service outcomes.
- **Data sharing and integration** has been an ongoing focus of the government. Recent progress includes the Consumer Data Right rollout, a new national regime for public sector data sharing and individual agency collaboration with the private sector such as the ATO's pioneering partnerships with software providers. Implementing a more comprehensive system for sharing and using health data (with appropriate data security and privacy safeguards), as well as for other government-funded services, would create new opportunities for data-enabled productivity gains.
- **Technical digital and data skills** are increasingly demanded not just in Australia's technology sector, but by businesses across all industries as economic and social activity becomes more digitised (particularly since COVID-19). Many formal and informal education and training options exist, with employers and workers already using these to meet their skill needs over time. Migration policy can also play a major role in providing skilled workers who have sophisticated digital and data capabilities developed overseas, and this policy may be used to address immediate workforce gaps or obtain skills that are difficult to develop locally.

Beyond these areas, community trust in new applications of technology is critical for future uptake, as businesses and governments need to maintain their social licence to deliver digital and data-enabled services. Many factors contribute to building trust, and two important aspects are having **secure and ethical digital and data practices**. But organisations sometimes underinvest in these areas; for example, smaller businesses in particular may lack the expertise to invest in cyber security, potentially creating broader vulnerabilities and undermining trust, which ultimately stymies adoption. Governments can play a role in supporting secure and ethical uses of technology and data — for instance by regulating high-risk settings — but intervention should be carefully balanced to avoid discouraging private sector investment and innovation.

Digital technology and data will continue to shape global economic growth and social change over the coming years. Whether Australia fully realises the productivity dividend arising from these opportunities depends on how effectively governments, businesses and individuals can recognise and safely harness these changes for our own benefit. This volume of the 5 Year Productivity Inquiry presents the Commission's findings and recommendations for government to support future data and digital activity.

1. Use of digital technology and data in the Australian economy

Key points

- **Digital technology and data have the potential to significantly improve Australia's productivity.**
  - Digital technology and data can reduce business production costs. Examples include lowering search costs (e.g. algorithmic search engines compared with manual search), transportation costs (e.g. using digital tools to generate and transmit data rather than paper records) and verification costs (e.g. establishing identity and reputation online instead of in person).
  - Greater use of digital technology and data can improve product quality and consumer choice, particularly in the services sector. Millions of phone apps, online banking, telehealth consultations, computer-assisted services such as counselling, and entertainment streaming services are examples of improved and/or new products enabled by technology and data.
- **Digital technology and data use has steadily increased for much of the past decade, as more businesses and consumers recognise the benefits of digitisation. COVID-19 accelerated this trend — many businesses were forced to operate only online, such as retailers making online sales, and more people worked from home.**
- **Businesses face benefits and costs from adopting digital and data tools that likely vary based on characteristics such as their size and industry. This could explain the variation in the rates at which technologies diffuse across the economy, and may affect dispersion in business performance.**
  - Larger businesses are more likely to adopt digital and data tools than small businesses.
  - Businesses in regional or remote areas are less likely than businesses located in cities to use customer relationship management and enterprise resource planning software.
  - The type of technology adopted and its relevance varies between industries. For example, knowledge intensive service businesses are more likely to use artificial intelligence (AI), while businesses in industries that are reliant on physical equipment are more likely to use radio frequency identification tags.
- **Compared with other developed countries, Australia does well on basic measures of technology and data uptake, but is falling behind on more advanced uses. This could limit future productivity growth.**
  - Australia has relatively high internet coverage and data download volumes.
  - Australia's internet speeds and use of AI and data analytics are relatively low.

1.1 Economic gains from using technology and data

Digital technology and data are two separate — though sometimes related — concepts.

- Digital technologies are electronic or computerised devices and systems that usually enable repetitive, and often time-consuming, operations to be undertaken more quickly (and sometimes more safely and robustly), such as through online or automated methods.
- Data refers to 'representations of facts that are stored or transmitted as qualified or quantified symbols. It comprises material such as characters, text, words, numbers, pictures, sound or video' (PC 2017a, p. 54).

The two are increasingly related because while data does not require technology (for example, a patient's medical history handwritten by their doctor on paper is still data), digital tools and systems have enabled large amounts of data to be gathered, stored, organised and analysed. Globally, the amount of digital data being generated is increasing at an incredible rate, with estimates that 'the present rate of digital content production is about 2.5 quintillion digital data bytes produced every day on Earth' (Vopson 2020, p. 1). Researchers observe that:

> … technology has lowered the cost of collecting, distributing and using data … [and] many firms are exploring and experimenting with these technologies. They can potentially generate many benefits for producers and users. (Duch-Brown, Martens and Mueller-Langer 2017, p. 4)

In this manner, digital technology and data often combine to create value: data's value is enhanced because of what can be done with it using technology; technology has value in part because its use can generate digital data and because of its role in storing, processing and analysing data.

There are a range of technologies that are causing, or have the potential to cause, rapid changes in the way our economy and society functions — both by virtue of the technology itself and because of what it enables us to do with data (box 1.1).

Box 1.1 – Examples of potentially transformative technologies

Cloud computing is the delivery of computing services (such as data storage, networking and analytics) over the internet. It allows users to access these services on demand, often via a 'pay-as-you-go' model, which improves flexibility and can lower costs.

Artificial intelligence (AI) is the ability of computers to simulate human intelligence and perform associated tasks (such as speech recognition, moving objects and strategic decision making) in an automated fashion. Machine learning is a type of AI in which a computer algorithm automatically improves its predictions through more data and experience.

Data analytics uses data to gain insights for decision making. The data can come from anywhere, such as consumer purchasing behaviour, weather events, the stock market, the human genome or student test scores. Data analysis can be as simple as calculating averages, or can involve complex methods like machine learning. It also involves producing predictive statistics and data visualisations.

Blockchain is 'a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network. An asset can be tangible (a house, car, cash, land) or intangible (intellectual property, patents, copyrights, branding)' (IBM nd). 'Web 3.0' aims to use blockchain technology to remove the centralised nature of the internet ('web 2.0') and increase security and trust.

Box 1.1 – Examples of potentially transformative technologies

The Internet of Things (IoT) involves 'connecting any device… to the Internet and to other connected devices. The IoT is a giant network of connected things and people – all of which collect and share data' (Clark 2016). Examples of IoT include connecting devices together in the home, using sensors to streamline production in a factory and using geolocated devices to improve road congestion.

Virtual reality uses computer simulation to allow users to interact with a virtual environment. Conversely, **augmented reality** superimposes digital images on the real world to facilitate interaction with the physical world. They can be used as interaction tools for digital twins to solve issues such as making human-robot collaboration safer (Pérez et al. 2020) or workflow problems (Havard et al. 2019).

Robotic process automation is the use of software that enables 'bots' to emulate human behaviour and complete automated tasks. This can be used in industries where simple and repetitive tasks can be automated such as data entry, addressing customer queries and automated internal communications. Bots are also finding applications in human services, such as for assessing healthcare consumers receiving care in their home (Medibank 2022).

3D printing is the process of creating solid objects from digital files. It can be used to create consumer and industrial products, as well as health products like dental implants and prosthetics.

Quantum computing utilises quantum mechanics to 'solve problems too complex for classical computers' (IBM nd). The exponential increase in computing power that quantum computing could offer would revolutionise AI and cyber security, make financial forecasting far more precise and vastly improve the efficiency of complex manufacturing (Bova, Goldfarb and Melko 2021).

How can digital technologies and data contribute to productivity?

Under a standard economic growth model, there are two main ways that digital technologies and the use of data contribute to the production process and therefore to economic activity. They can be thought of as direct inputs to the production process or as part of the 'residual' portion of output growth that cannot be attributed to capital or labour inputs.

Businesses can invest in digital technologies as capital inputs, including physical and tangible capital such as computer hardware, as well as intangible inputs such as software programs and ways to collect, store and analyse data. This capital is then used to produce goods and services — for example, a retailer uses their computer systems to manage supplier and customer orders, or a bank applies an algorithm to customer data to inform their loan assessment. Investing in digital technologies as capital inputs can substitute for labour inputs (such as by automating tasks previously done by workers), complement existing labour (for example, time-saving digital tools allow workers to do more value-adding tasks) or create different processes or outputs requiring more labour or new skills.

The classical economic production function sometimes refers to the residual, after capital and labour have been accounted for, as 'technology' (instead of 'total factor productivity'). This concept is broader than the examples outlined in box 1.1 and captures the effects of all manner of technologies including 'general purpose technologies', which are 'characterized by the potential for pervasive use in a wide range of sectors and by their technological dynamism' (Bresnahan and Trajtenberg 1995). While computers and the internet are examples of such technologies, others predate the recent digital revolution and include the steam engine and electricity (Lipsey,

Carlaw and Bekar 2005). Such technology improvements can have a multiplier effect on output by increasing the productive potential of an economy for a given amount of capital and labour inputs. They can also facilitate complementary innovations; for example, computers are used for purposes well beyond their original function of performing complex mathematical calculations (Brynjolfsson and Hitt 2000).

Data is a unique input because, unlike most other production inputs such as materials and equipment, it is 'non-rivalrous': many agents can make use of the same data at the same time without it being "used up" or degraded (Smedes, Nguyen and Tenburren 2022, p. 3). This means that data can make a larger economic contribution than more traditional inputs, as multiple businesses can use the same data to produce different outputs. Research has found that businesses reporting the greatest growth in revenue and earnings received a significant proportion of that boost from data and analytics, with high-performing organisations three times more likely than others to say their data and analytics initiatives have contributed at least 20% to earnings before interest and taxes over the past three years (McKinsey 2019).

However, in many cases data can be made 'excludable' — it is usually the way that data is stored and accessed that determines whether other parties can be excluded from using it. For example, data may be encrypted or a private entity that collects data may choose not to share it for others to use. Sometimes this is desirable because it provides incentives for collecting data, such as businesses gathering customer data to improve their products and gain a competitive advantage. At the same time, excluding others from accessing and using data can mean that the value of data as an input to the production process is not fully realised (section 2.2).

In addition to their role as production inputs, both digital technology and data can be considered as the outputs of production in some contexts. For example, software companies produce digital applications as their output, which can either be sold directly to consumers or used as inputs by other businesses that wish to automate their processes but do not have the technological capabilities to create their own applications. And the media content produced by streaming services represents data that is these companies' output — with a consumer's selection of which content they view, becoming data used by companies as an input to preview future content for that consumer.

Better use of technology and data can improve productivity …

Businesses can use digital tools, often in combination with data, to reduce their production costs, although this may not immediately translate to productivity growth due to lags in price adjustments (Basu, Fernald and Kimball 2006). Various researchers have found positive relationships between technology adoption and productivity or GDP growth (box 1.2), and Goldfarb and Tucker (2019) outline a range of channels through which technology can lower businesses' costs.

- Search costs — the internet makes it easier to find information and therefore lowers search costs for both customers and businesses. Moreover, algorithmic search engines use data to improve the relevance and accuracy of search results, further reducing these costs.
- Replication costs — processes using digital technologies can have low marginal costs after the fixed costs of development and implementation are incurred. For example, a bank that invests in technology to support its risk assessments can readily scale this across multiple customers and products.
- Transportation costs — there are near-zero costs associated with transporting digitised data over the internet, compared with higher costs of transporting (for example) paper-based records. This also has implications for the location of people, as technology enables geographically isolated individuals and companies to connect at lower cost, facilitating new employment models such as offshoring.
- Tracking costs — digital tools can help businesses to keep track of relevant data from customers and suppliers at lower cost, though better tracking has also made privacy a key issue. Analysing this data can help businesses to streamline production or distribution.

- Verification costs — technology and new data sources can make it easier to verify the identity and reputation of another party in a business transaction, so that it is less costly to build trust between parties (for example, less need for repeated interactions).

Box 1.2 – Technology and productivity: empirical evidence from previous research

Studies from a range of countries have found a positive relationship between technology adoption and productivity or GDP growth. In several cases, the evidence suggests that the economic benefits from using technology are larger for businesses that have also invested in complementary areas, such as management capabilities and data assets.

- Gal et al. (2019) looked at the effect of technology adoption on productivity in 19 EU countries and Turkey, finding that 'an industry environment characterised by high digital adoption rates is associated with higher [multifactor productivity] growth in the average firm' (Gal et al. 2019, p. 18). The research also found evidence that the gains from digital technology are dependent on 'intangible assets and skills (e.g. data, tacit knowledge, organisational capital) and complementary additional investments in these factors' (Gal et al. 2019, p. 31).
- Vu (2013) examined the impact of ICT on Singapore's GDP and average labour productivity (ALP) growth. The research found that 'ICT capital played a substantial role in Singapore's growth, contributing 1.0 percentage point to GDP growth and 0.8 percentage points to ALP growth in 1990-2008' (Vu 2013, p. 18).
- Bloom, Sadun and Reenen (2012) investigated the relationship between technology and labour productivity for multinational companies. Doubling the IT stock was associated with a 6.3% labour productivity increase for US multinationals and 4.6% for non-US multinationals (Bloom, Sadun and Reenen 2012, p. 180). The researchers also demonstrated that the higher productivity gains for US multinationals were attributable to better management practices, which complemented IT investment.
- Borowiecki et al. (2021) studied the effects of digitisation on firm productivity in the Netherlands, finding positive and significant productivity impacts from investment in ICT hardware and intangibles (as measured by levels of digital skill intensity). Their results held using both labour productivity and multifactor productivity as the measure of productivity.
- Qu, Simes and O'Mahony (2017) examined the relationship between economic activity and technology use, measured through internet access and mobile phone penetration, in 37 countries. They found that from 2004 to 2014, after controlling for other inputs such as physical and human capital, 'the diffusion of digital technologies significantly improved economic output in Australia and abroad, contributing to steady-state gross domestic product per capita growth of approximately 5.8% on average [over the whole decade]' (Qu, Simes and O'Mahony 2017, p. 57).

The capacity of businesses to use new technologies and the impact on their performance varies with their characteristics and capabilities, which leads to heterogenous uptake of digital technology and data use (discussed in more detail below). The complex variety of benefits that can stem from using multiple technologies in combination also contributes to this heterogeneity; as do differences in the nature of the available data that can be analysed using digital tools.

For example, industries that make greater use of equipment could be more likely to benefit from the Internet of Things (IoT) and sensors integrated into their equipment, such as resources companies using sensors to gather real-time data on their machinery to improve maintenance and operational performance (PMC 2021c,

p. 7). Technology has lowered the costs of gathering and transporting information, as well as the costs of tracking and monitoring their equipment. In contrast, industries that are centred on human decision making might be more likely to find applications for AI, such as banks investing in bill management algorithms or automating qualifying decisions on new customers and their loan limits (Agarwal, Singhal and Thomas 2021; CBA 2022). In these examples, technology has lowered the cost of verifying the customer information underpinning these decisions, and reduced replication costs for making these decisions across many customers.

This is not to say that particular technologies are exclusively used by businesses in specific industries; however, it does suggest that what data and digital adoption looks like will vary across the economy. Australian businesses' adoption of different data and digital tools and how this differs across industries is further examined below.

Real cost reductions are not the only way that digital and data enabled productivity improvements benefit Australians. The fruits of productivity growth can also be experienced as quality improvements – the things that get better (in measured and unmeasured ways); and new things – inventions so novel that they can be said not to have existed before and perhaps were not even conceived of by most people, but that create new value for society (Brennan 2021).

New uses of technology and data often lead to product improvements and greater choice, particularly in the services sectors, which have historically had more difficulty achieving productivity growth. Digitisation can create novel ways for customers to interact with businesses and service providers (such as online banking, telehealth consultations and computer-assisted services such as counselling) or even entirely new products (such as social networks, search engines, phone apps and streaming entertainment). Sometimes the main enabler of improvements is technology-driven cost reductions through one or more of the channels discussed above. In other instances, the key enabler is better use of data; the channels through which data itself provides economic benefits are discussed in section 2.2. Many significant changes have resulted from a combination of both, with the digitisation of data enabling benefits on a larger scale.

For example, the digital tools that have enabled businesses to track customer data at lower cost can also provide the means for businesses to offer more personalised goods and services that are tailored to an individual customer's needs. This results in a better-quality product for the customer while also sharpening allocative efficiency by improving business decision making about resource allocation. In this example, the substantial value that can be gained from collecting and analysing this data provides the rationale for many retailers to offer loyalty programs, some of which can span multiple product categories.

Finding 4.1
Technology and data are enablers of productivity growth

Digital technology, combined with data, can help businesses to improve their productivity by lowering the costs of search, replication, transportation, tracking and verification. It can also lead to productivity-enhancing product improvements and greater choice, particularly in services sectors, which have historically had more difficulty achieving productivity growth.

… but measuring the digital economy is challenging

Given the many potential benefits of digital technologies and their applications in creating value from data, they are ubiquitous in one form or another throughout every part of Australia's economy.

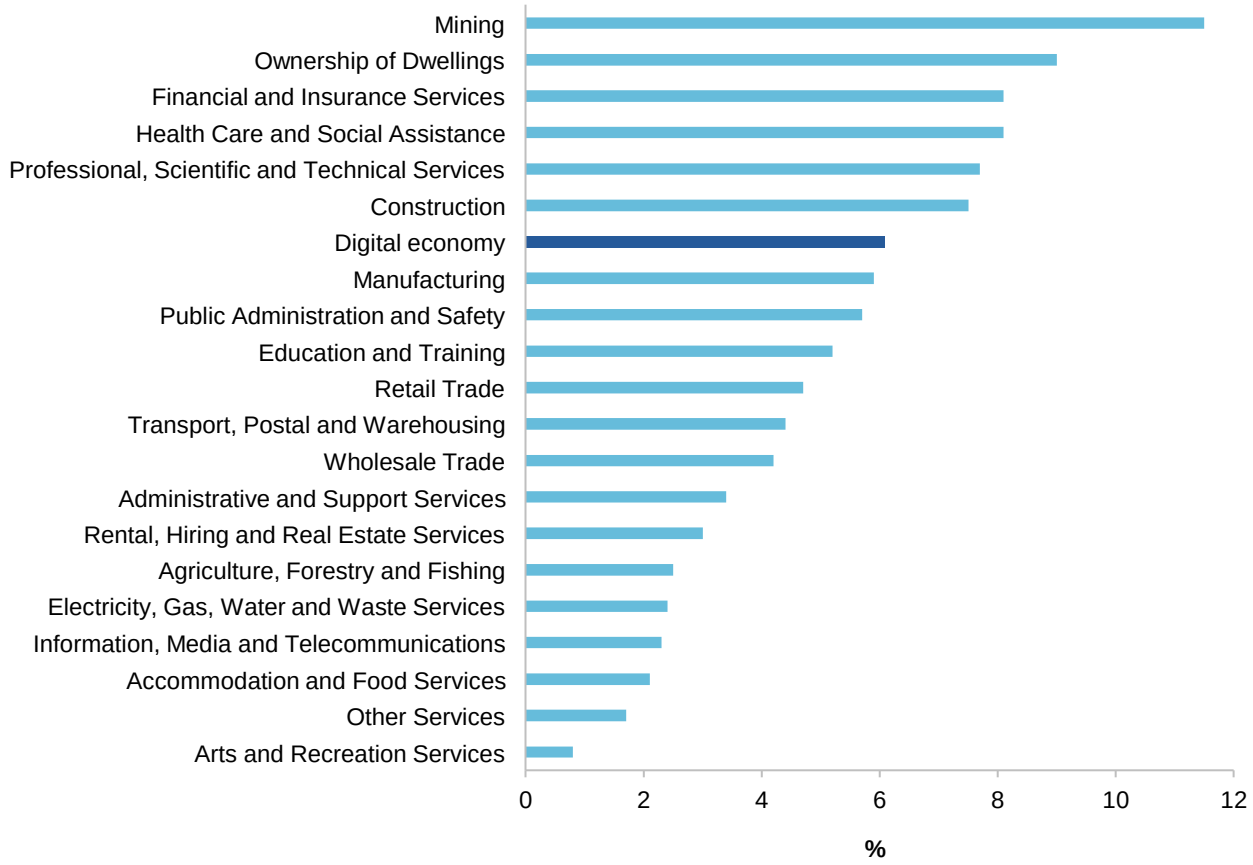
There are many jobs, products and processes that can be identified as digital activities — such as IT support, computer product manufacturing and developing software. Taking together these observable components, the ABS reports that digital activities make a large economic contribution, representing about 6% of total value added in 2020-21 (figure 1.1). However, this is an underestimate of the economic value of digital technologies. The ABS's estimates reflect the output associated with products that are 'primarily digital in nature', but do not measure the economic value attributable to the ubiquitous and embedded use of technology in other products. For example, much of the mining industry's output depends on digital technology — Rio Tinto's Gudai-Darri mine in the Pilbara is one of the most technologically advanced in the world. It uses 'autonomous trucks, trains and drills, as well as the world's first autonomous water trucks, and a robotic ore sampling laboratory' (MCA 2022, p. 11).

Other estimates of the size of Australia's digital economy, or the contribution of technology to the economy, range from being similar in magnitude to ABS estimates in figure 1.1, to far in excess of these. These variations are partly attributable to differences in how digital technologies are conceptualised and how their impacts are measured.

- AlphaBeta examined the technology sector's contribution to Australia's GDP both directly — through industries such as internet publishing and computer system design, and internet related profit shares in wholesale and retail trade — and indirectly — based on estimating the share of profits and wages in other industries attributable to technology. They estimated that, combining direct and indirect contributions, the technology sector represents 6.6% of GDP (AlphaBeta 2019a, p. 11).
- The Tech Council of Australia estimated that technology sector activity contributed $167 billion to Australia's GDP in 2020-21, representing 8.5% of Australia's total economic output (TCA, sub. 51, p. 1). Its estimates capture segments of the information media and telecommunications; professional, scientific and technical services; retail trade; and wholesale trade industries, which it observes have all outpaced average market sector industries' multifactor productivity growth in the decade to 2020-21 (TCA, sub. 51, p. 2).
- Oxford Economics and Huawei considered digital spillovers, which happen 'when technology accelerates knowledge transfer, business innovation, and performance improvement within a company, across supply chains and amongst industries' (Huawei and Oxford Economics 2017, p. 24). They estimated that digital spillovers could account for 13.1% of GDP in advanced economies.
- McKinsey estimated gains from the digital economy by examining technology-enabled cost reductions in particular industries — for example, that electronic medical records produced a 25% reduction in avoidable hospital readmission rates, and a 20% reduction in length of stay (Blackburn, Freeland and Gärtner 2017, p. 34) — then projecting the implications of increased digital adoption. They reported that digital technology has 'the potential to contribute between AU $140 billion and AU $250 billion to Australia's GDP by 2025, based on currently-available technology alone… [representing] an aggregate GDP increase over historical trend of roughly 10 percent by 2025' (Blackburn, Freeland and Gärtner 2017, p. 2,13).

Figure 1.1 – Digital activities represent 6% of Australia's total value added[a,b]

Share of total value added by Australian industries (at current prices and with digital activity embedded), 2020-21[c]



a. Digital activity is measured as the production of: computer hardware, software, telecommunications equipment and support services that form and facilitate the use of computer networks; digital audio, video and advertisement broadcasting services that can be created, accessed, stored or viewed on digital devices; and retail and wholesale services and margins from digitally ordered or platform enabled online transactions. **b.** For simplicity, the measurement focused on products that were 'primarily digital' in nature, and separately identifiable in the supply-use tables. **c.** The production of the digital products has not been removed from the existing industries for which it is partially embedded. Therefore, the shares add to more than 100% of aggregate value added.

Source: ABS (2022b).

Businesses' use of technology and data has been increasing

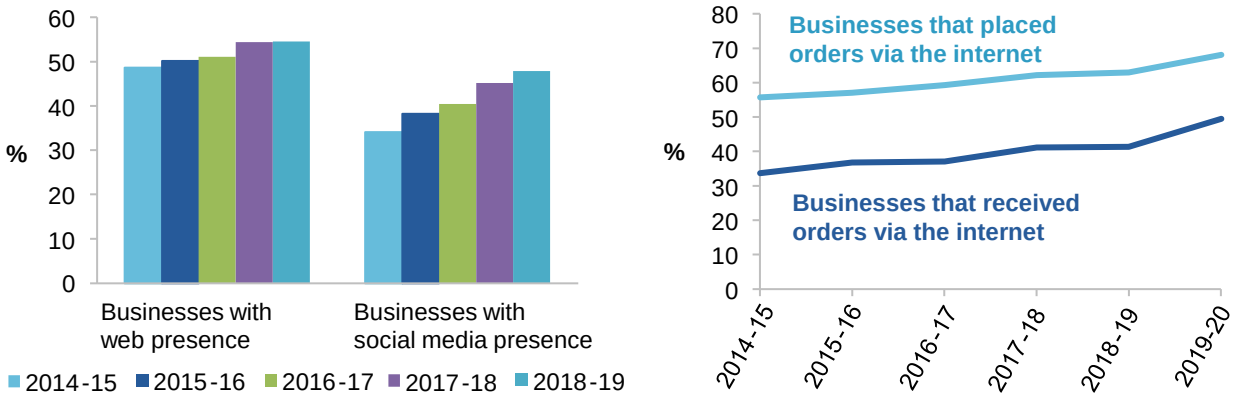
The rising adoption of digital technologies reflects their direct economic benefits to businesses, but also the fact that most businesses cannot be part of the business ecosystem without digital tools. Merely achieving compliance with tax and many other regulations requires technology and, as such, almost all businesses have access to the internet.[1] And for many businesses, a web presence is essential to reaching customers: between 2014 and 2019, the share of businesses with a web presence increased from about 49% to 55%, and the share of businesses using e-commerce to either receive or place orders has also been rising (figure 1.2).

[1] Over 95% of Australian businesses had internet access in 2016-17, of which over 99% reported using broadband internet (ABS 2018).

Data download volumes have also increased significantly over recent years. According to the ACCC's *Internet Activity Report*, 11.6 million terabytes of data were downloaded across retail broadband internet and mobile services in the June 2022 quarter, up 94% from June 2019 (figure 1.3).

Figure 1.2 – Australian businesses increasingly operate online

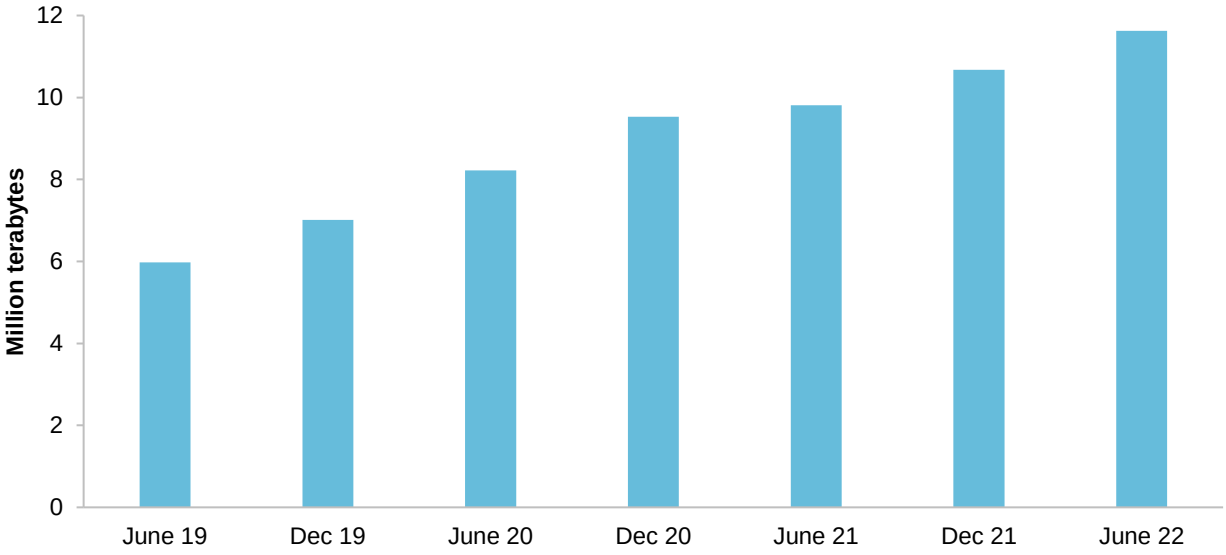
Share of businesses with online presence, 2014-15 to 2018-19, and using e-commerce, 2014-15 to 2019-20



Source: ABS (*Characteristics of Australian Business,* 2019-20 financial year, Cat. no. 8167.0; *Business Use of Information Technology*, 2015-16 financial year, Cat. no. 8129.0; *Summary of IT Use and Innovation in Australian Business*, 2016-17 financial year, Cat. no. 8166.0).

Figure 1.3 – Data download volumes are rapidly growing

Total volume of data downloaded for retail NBN, retail non-NBN fixed and mobile services, June 2019 to June 2022



Source: ACCC (2022f).

COVID-19 and working from home accelerated digital uptake

Most recently, COVID-19 has accelerated technology use as many parts of the economy have had to conduct business online during the pandemic. This includes knowledge-based organisations transferring their existing digital processes from office-centric to online, retailers augmenting their physical sales with online sales, and various services being delivered digitally — for example, the COVID-19 pandemic necessitated a more rapid transition to eHealth, including online general practitioner (GP) consultations for routine medical services (KPMG, sub. 60, p. 14). The Australian Government's Digital Economy Strategy 2030 highlighted that almost 9 in 10 Australian businesses adopted new technologies during COVID-19 to support business continuity (PMC 2021c, p. 5).

Much of this technology adoption was necessary to allow workers (about 40% of Australia's workers) and businesses to operate from home (PC 2021c). The pandemic demonstrated that many jobs could be done from home just as well as from a traditional employer-owned location — such as office-based workers and jobs where workers use computers and other portable technology, rather than working with immovable structures, materials or equipment. Had this not been the case (that is, had the proportion of businesses and workers able to take up digital technologies to operate online and remotely been much smaller), Australia's economic activity and productivity would likely have taken a greater hit as a result of COVID-19 restrictions. According to an international analysis of workers' digital communication patterns, during the 2020 lockdowns the length of the average workday increased by about 8.2% relative to pre-pandemic levels, or almost 49 minutes (DeFilippis et al. 2020).

Although the long-term outcomes are unclear, the amount of work done from home is likely to remain much higher than it was before the pandemic. As COVID-19 restrictions have eased, hybrid work (with a portion of the week at home and a portion at the employer's site) has become a regular and expected part of many workplaces. Hybrid work comes with a variety of upsides and downsides for businesses and employees (PC 2021c). In terms of digital technologies, hybrid work may increase ongoing capital expenditure on equipment for home offices, such as laptops, headphones and software (including for videoconferencing and webinars). Businesses may also increase their investments in digital infrastructure, its maintenance and training in its use, to enable remote working to continue in tandem with activity at a workplace.

As firms and workers learn more about how to effectively work from home, the productivity and wages of those doing so are likely to improve. Those arrangements that facilitate higher productivity when working from home and in workplaces are likely to become more prevalent through the process of innovation and learning — via changing technology and business practices — albeit at an uncertain pace. Technological progress could be combined with the lessons from experimenting with different approaches to remote work, which would further reduce the costs of working from home. Better ways of facilitating collaboration and creativity could be found, mitigating the downsides of working from home on productivity. In addition, digital technology could give a broader range of occupations and industries the option of remote work, for all or part of their regular hours worked. More firms might move to being fully remote, but considerable momentum would likely come from firms moving from a fully centralised to hybrid model (or increasing the levels of work from home within hybrid models).

Uptake of foundational versus specialised technologies

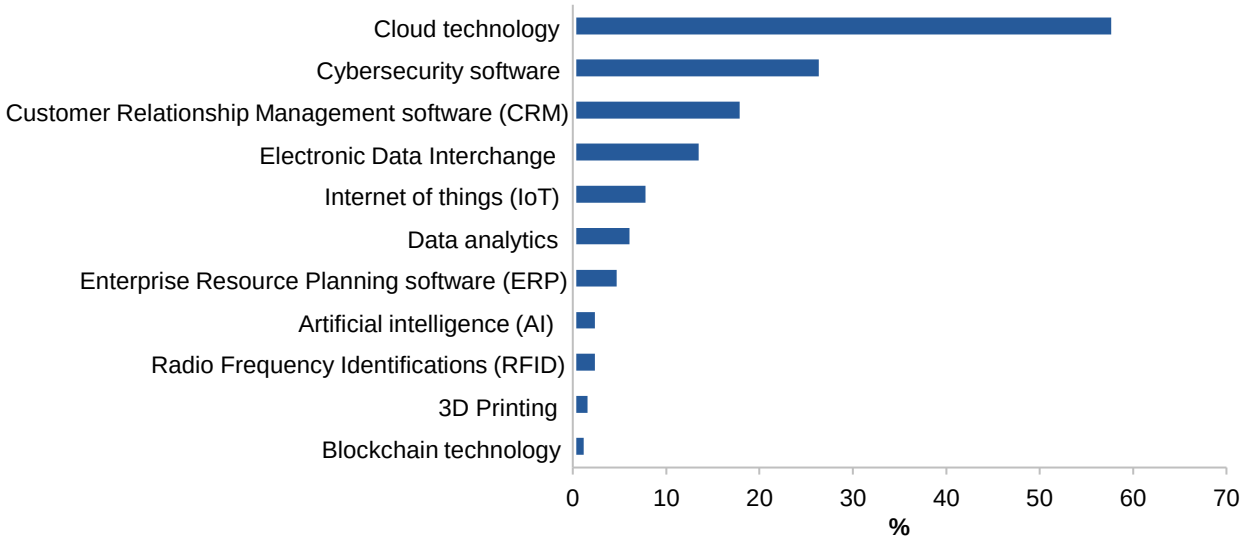
The level of technology uptake by Australian businesses varies across different types of digital and data tools. Adoption is typically higher for technologies that are foundational and have broader uses across a range of business applications. For example, 57% of Australian businesses reported using cloud technology

in the ABS's 2019-20 *Business Characteristics Survey*,[2] and more than one quarter of businesses reported using cyber security software (figure 1.4).

These foundational technologies have widespread applications and are often necessary to have in place when adopting more advanced types of digital and data tools. More specifically, cloud-based software can lead to significant productivity improvements in and of itself; for example, TechnologyOne submitted that 'a transition to consumption-based software [or cloud-based software-as-a-service] across key sectors over the next three years could realise $224 billion in savings and uplift GDP by 1.3 percent above the base in 2030 (assuming a 2022 start date)' (TechnologyOne, sub. 66, p. 2). On average, 54% of these gains came from productivity-enhancing business process improvements and 32% from reduced technology costs.

Figure 1.4 – Technology uptake is higher for foundational tools

Share of businesses using different ICTs, 2019-20[a]



a. This chart uses weighted estimates as published by the ABS.

Source: ABS (*Characteristics of Australian Business,* 2019-20 financial year, Cat. no. 8167.0).

Technologies that are relatively niche, require significant investment in equipment or labour to enable uptake, or are more complex to understand their potential benefits and use generally have lower business adoption. To the extent that these technologies have a narrower set of economic applications at present, it may be optimal for current take-up rates to be relatively low. These include 3D printing and blockchain, which were each reported to be used by about 1% of Australian businesses in 2019-20 (figure 1.4). Some other tools that either generate or require large volumes of data to be used effectively, such as artificial intelligence (AI), analytics and IoT, also had relatively low uptake.

The various factors that can lead to lower technology adoption by Australian businesses — for example cost, lack of staff capability and uncertainty about benefits — are discussed in section 2.1. In addition, the Business Characteristics Survey is self-reported data; therefore, its results on technology adoption partly reflect businesses' understanding of how they are using digital and data tools. This may be an underestimate if businesses do not recognise that they are using some forms of technology. For example, most Australian

[2] The Business Characteristics Survey is an annual survey that provides 'estimates in business use of information technology; innovation; and a broad range of other non-financial business characteristics' (ABS 2021b). The 2019-20 survey captured business conditions prior to COVID-19 and also during the start of the pandemic, as parts of Australia entered lockdown in early 2020.

businesses would make use of electronic data interchanges as tax returns are submitted electronically; however, some may not recognise this when responding to the survey. Similarly, businesses may indirectly use AI if it is embedded in their third-party software, but may not think to report this.

Adoption of technology is not the only condition required for businesses to get productivity benefits from digital and data tools. To maximise value, digital investments have to be integrated into a business's processes and broader production model. Poorly integrated technology can lead to duplication and additional costs; for example, a MYOB survey of small and medium enterprises found that surveyed businesses wasted, on average, 7 hours per week due to lack of integration, with this time spent on manual data entry, consistency checks or fixing errors (MYOB 2022, p. 5). In some cases, the frustrated business simply ditched its digital investment. These experiences further highlight the importance of skills, support and ease of integration for improving processes and subsequent technology uptake.

Finding 4.2
Australian businesses are increasingly using technology

Most Australian businesses make some use of digital tools, such as having a web presence, placing orders online and adopting cloud technology. COVID-19 accelerated technology use, with many businesses shifting to online sales or digitally delivered services. Technology adoption is highest for foundational tools such as cloud technology and cyber security software. To the extent that some technologies (such as 3D printing and blockchain) may have a narrower set of economic applications, it could be optimal for take-up rates to be relatively low at present.

Different adoption rates likely reflect heterogenous benefits and costs

There is variation in adoption rates for each type of technology, depending on business characteristics. As discussed above, heterogenous uptake of digital and data tools is to be expected because businesses of different sizes and industries are likely to derive different benefits and costs from using a specific technology. This in turn affects how quickly or slowly a given technology diffuses across Australian businesses which, given the evidence suggesting a positive relationship between technology adoption and productivity (box 1.2), could affect the dispersion of business performance across the economy. The Commission found that, holding all other characteristics constant:[3]

- larger businesses were significantly more likely than smaller businesses to have adopted digital and data tools across almost all surveyed technologies, with uptake being highest among the largest businesses with 200 or more employees. Consistent with this, the Australian Small Business and Family Enterprise Ombudsman has stated that 'small business managers are not always as supportive of technology adoption compared to larger businesses' (ASBFEO, sub. 64, p. 3)

[3] To understand the business characteristics driving differences in technology adoption, the Commission has undertaken regression analysis using the ABS's *Business Characteristics Survey* data. Logistic regressions were estimated to identify which characteristics were relatively more important for explaining digital and data uptake across the 11 technologies that businesses were surveyed about in 2019-20. The variations reported here are for characteristics estimated to be statistically significant at the 5% level, holding all other characteristics constant (for example, the results on varying location are after controlling for business size and industry). Further details about the regression specification and results tables are provided in appendix A.

- businesses in regional and remote Australia were significantly less likely than businesses located in cities to use customer relationship management and enterprise resource planning software. However, business location generally had limited explanatory power in affecting other types of technology uptake
- there were many statistically significant variations in how businesses across different industries adopted different technologies.

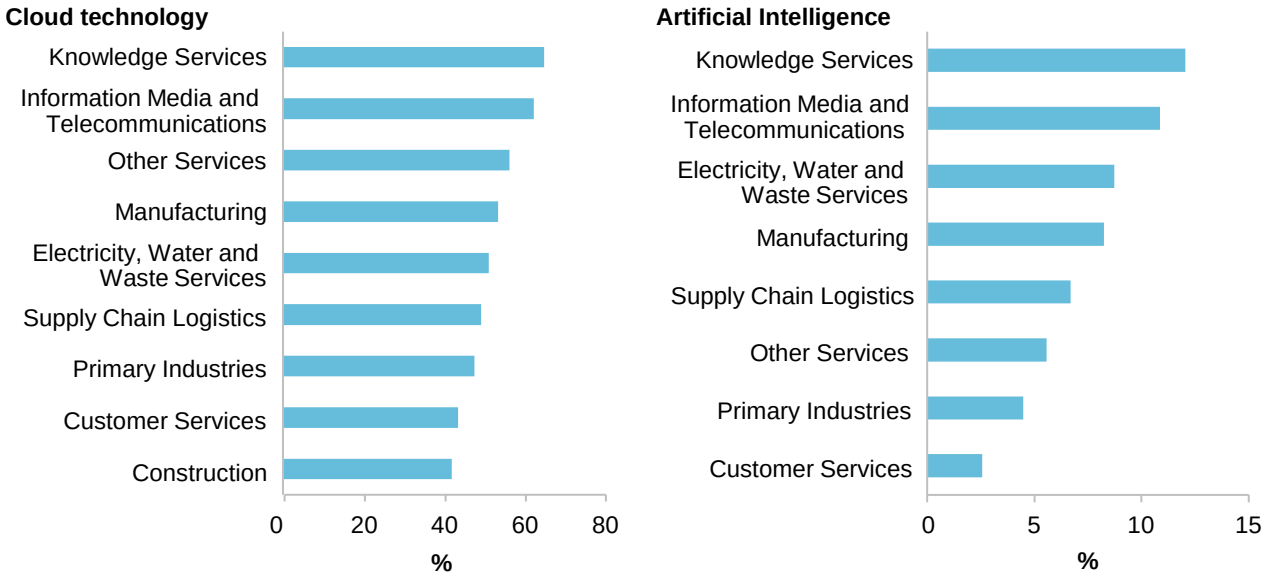
Businesses in knowledge services and information media and telecommunications were more likely to use cloud technology, with over 60% adoption by businesses within these industries in 2019-20 (figure 1.5). These industries are relatively knowledge intensive and require use of digital tools and computing power to produce outputs, and are therefore well-placed to benefit from using cloud technology. At the same time, even in industries with relatively lower cloud uptake, the adoption rate, in absolute terms, is still substantial — about 40% of businesses in construction and customer services use cloud technology.

This likely reflects the broader benefits of cloud technology as it has many basic applications that are relevant for all industries, such as storing and accessing information, as well as more complex uses that may be more relevant for knowledge-intensive industries, such as to access more processing power and enable the use of other technologies such as AI or data analytics. Previous research has found that a higher proportion of businesses adopt cloud technology for basic uses, such as software applications and data storage, reflecting the early stage of adoption by many businesses — but that cloud services will also have a foundational role in enabling next wave technologies (DAE 2019b, p. 4).

Consistent with this, industries with higher uptake of cloud technology also had higher adoption of AI. Businesses in the knowledge services and information media and telecommunications industries were more likely to be using AI, with adoption rates of more than 10% in 2019-20 (figure 1.5). Businesses that have been early adopters of AI are likely to have been those that stand to gain significant benefits from their use. A 2019 industry survey found that 56% of AI early adopters in Australia believe AI is very or critically important to their company's success now, and 79% believe this will be the case within two years (Deloitte Insights 2019, p. 8,10).

Figure 1.5 – Cloud and AI have higher adoption in knowledge-intensive industries

Share of businesses using selected technologies by industry, 2019-20[a,b,c]



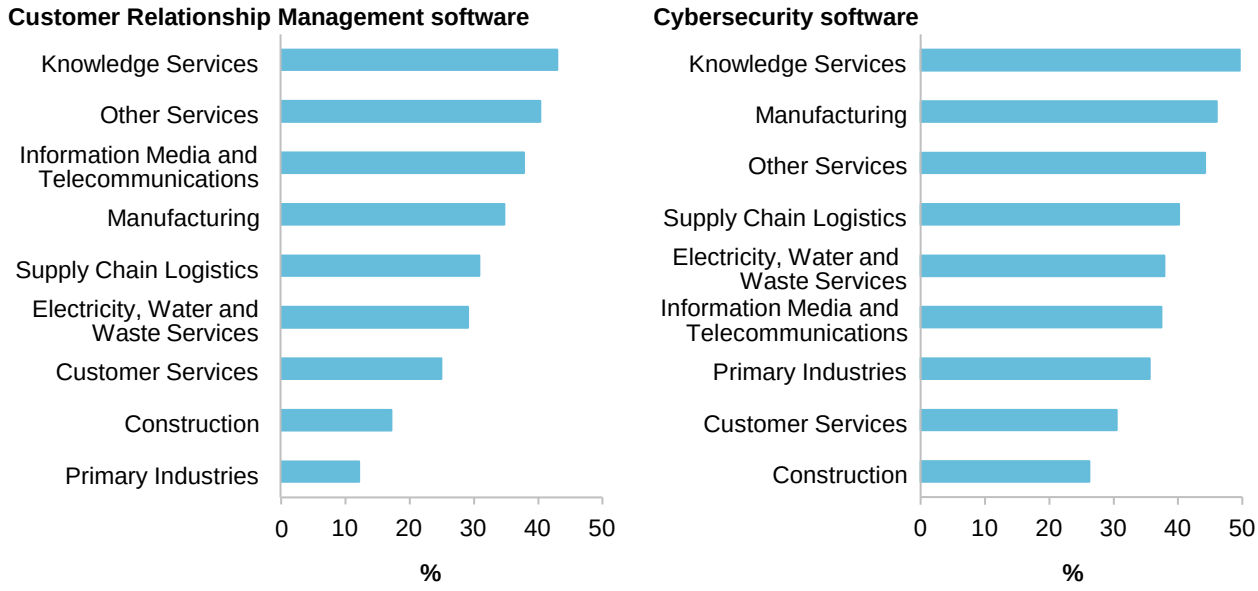
a. Some ANZSIC 2006 divisions have been grouped for this analysis. 'Customer services' includes retail trade; accommodation and food services; and other services. 'Knowledge services' includes finance and insurance services; and professional, scientific and technical services. 'Other services' includes administrative and support services; healthcare and social assistance; arts and recreation services; and rental, hiring and real estate services. 'Primary industries' includes agriculture, forestry and fishing; and mining. 'Supply chain logistics' includes wholesale trade; and transport, postal and warehousing. The Business Characteristics Survey does not capture businesses in the Education and Training and Public Administration and Safety industries. **b.** These results are unweighted so are not directly comparable with the weighted estimates in figure 1.4. **c.** Construction industry adoption of AI unable to be reported due to sample size constraints.

Source: Productivity Commission estimates using data in the ABS's Business Longitudinal Analysis Data Environment.

Knowledge services businesses were also the most likely out of all industries to adopt customer relationship management (CRM) and cyber security software in 2019-20 (figure 1.6). Use of these digital tools by businesses in other industries varied substantially, potentially reflecting the complexity of their customer interactions (for CRM software) and their vulnerability to or awareness of cyber security risks (for cyber security software). However, some businesses may be underinvesting in cyber security due to underestimating the likelihood or total costs of a security breach, as discussed in section 2.2.

Figure 1.6 – Knowledge services businesses are the largest adopters of CRM and security software

Share of businesses using CRM and cybersecurity software by industry, 2019-20[a,b]



a. Some ANZSIC 2006 divisions have been grouped for this analysis. 'Customer services' includes retail trade; accommodation and food services; and other services. 'Knowledge services' includes finance and insurance services; and professional, scientific and technical services. 'Other services' includes administrative and support services; healthcare and social assistance; arts and recreation services; and rental, hiring and real estate services. 'Primary industries' includes agriculture, forestry and fishing; and mining. 'Supply chain logistics' includes wholesale trade; and transport, postal and warehousing. The Business Characteristics Survey does not capture businesses in the Education and Training and Public Administration and Safety industries. **b.** These results are unweighted so are not directly comparable with the weighted estimates in figure 1.4.

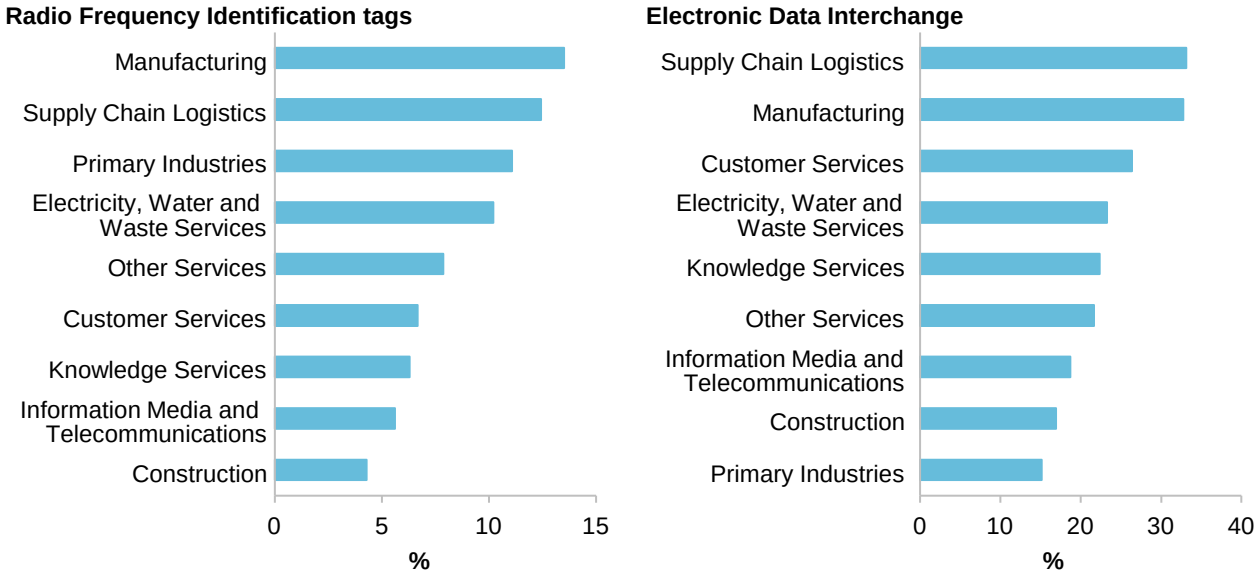
Source: Productivity Commission estimates using data in the ABS's Business Longitudinal Analysis Data Environment.

Businesses in the manufacturing, supply chain logistics and primary industries were more likely than others to use radio frequency identification (RFID) tags (figure 1.7). Higher adoption in these industries is likely to reflect the relatively greater gains to these businesses from using RFID tags to automatically identify and track objects. As discussed above, industries that make greater use of equipment — or have more requirements to physically move inputs and outputs as part of their production processes — are better placed to benefit from the cost reductions associated with this type of technology. There is significant potential for economic gain; for example, according to the Minerals Council of Australia, 'adoption of digital and technological innovation has the potential to deliver significant productivity improvements of up to 23% to the Australian mining industry by 2030' (MCA, sub. 55, p. 17).

Supply chain logistics and manufacturing businesses also have relatively higher uptake of electronic data interchange (EDI) tools, an established technology that includes real-time computer-to-computer exchange of transaction data such as invoices and purchase orders (figure 1.7). This is consistent with EDI enabling more efficient tracking of inputs and suppliers, and outputs and customers, which is particularly valuable for industries with complex production workflows and linkages, so they can lower costs and optimise decision making across their systems and processes (Min 2000).

Figure 1.7 – Manufacturing and supply chain logistics industries have the highest adoption of RFID tags and EDI tools

Share of businesses using RFID tags and EDI by industry, 2019-20[a,b]



a. Some ANZSIC 2006 divisions have been grouped for this analysis. 'Customer services' includes retail trade; accommodation and food services; and other services. 'Knowledge services' includes finance and insurance services; and professional, scientific and technical services. 'Other services' includes administrative and support services; healthcare and social assistance; arts and recreation services; and rental, hiring and real estate services. 'Primary industries' includes agriculture, forestry and fishing; and mining. 'Supply chain logistics' includes wholesale trade; and transport, postal and warehousing. The Business Characteristics Survey does not capture businesses in the Education and Training and Public Administration and Safety industries. **b.** These results are unweighted so are not directly comparable with the weighted estimates in figure 1.4. **c.** Electricity, Water and Waste Services. **d.** Information Media and Telecommunications.

Source: Productivity Commission estimates using data in the ABS's Business Longitudinal Analysis Data Environment.

Finding 4.3
Businesses in different industries adopt different digital tools

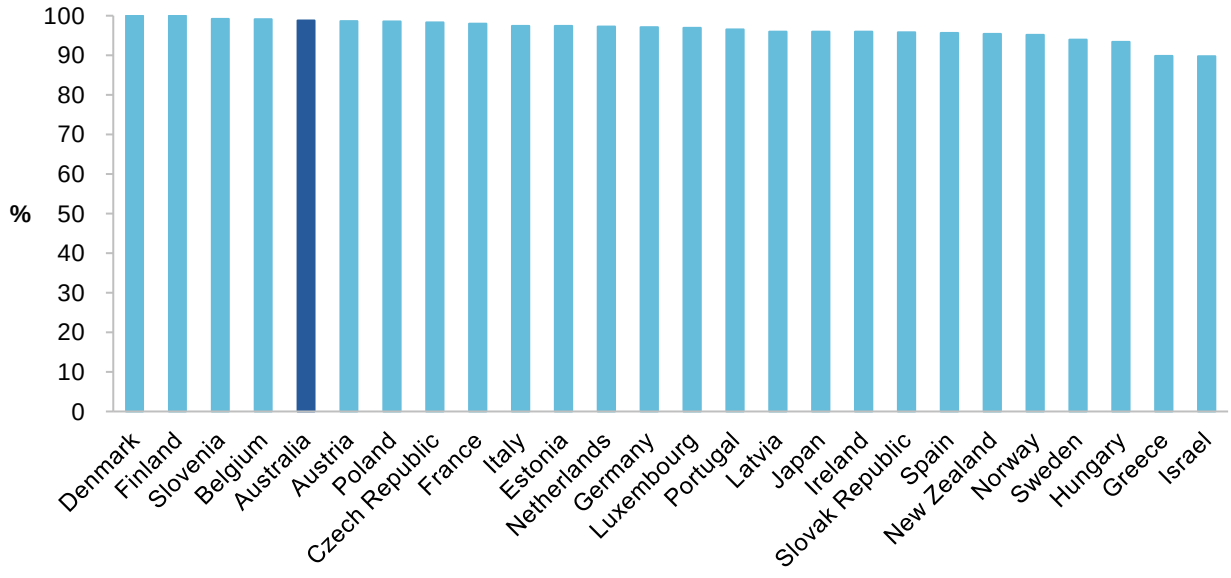
Variation in businesses' adoption of digital and data tools likely reflects differences in expected benefits and costs from adoption. For example, knowledge-intensive industries are more likely to use cyber security software and artificial intelligence, while manufacturing and supply chain logistics industries are more likely to use radio frequency identification and electronic data interchange tools. This could explain variation in the rates of technology diffusion across the economy and may affect dispersion in business performance.

1.2 International comparisons on technology and data use

Australia's internet coverage is high, but speeds are relatively low

Individual and business access to the internet is a useful starting point to understanding how Australia compares to other countries on digital and data use, as internet connectivity underpins most other technologies and their potential productivity benefits. Australian businesses are well connected to the internet relative to other OECD countries, with about 99% of Australian businesses having a broadband connection (either fixed or mobile) in 2020 (figure 1.8).

Figure 1.8 – Almost all Australian businesses have broadband internet connections
Share of businesses with a broadband connection (includes fixed and wireless), 2020



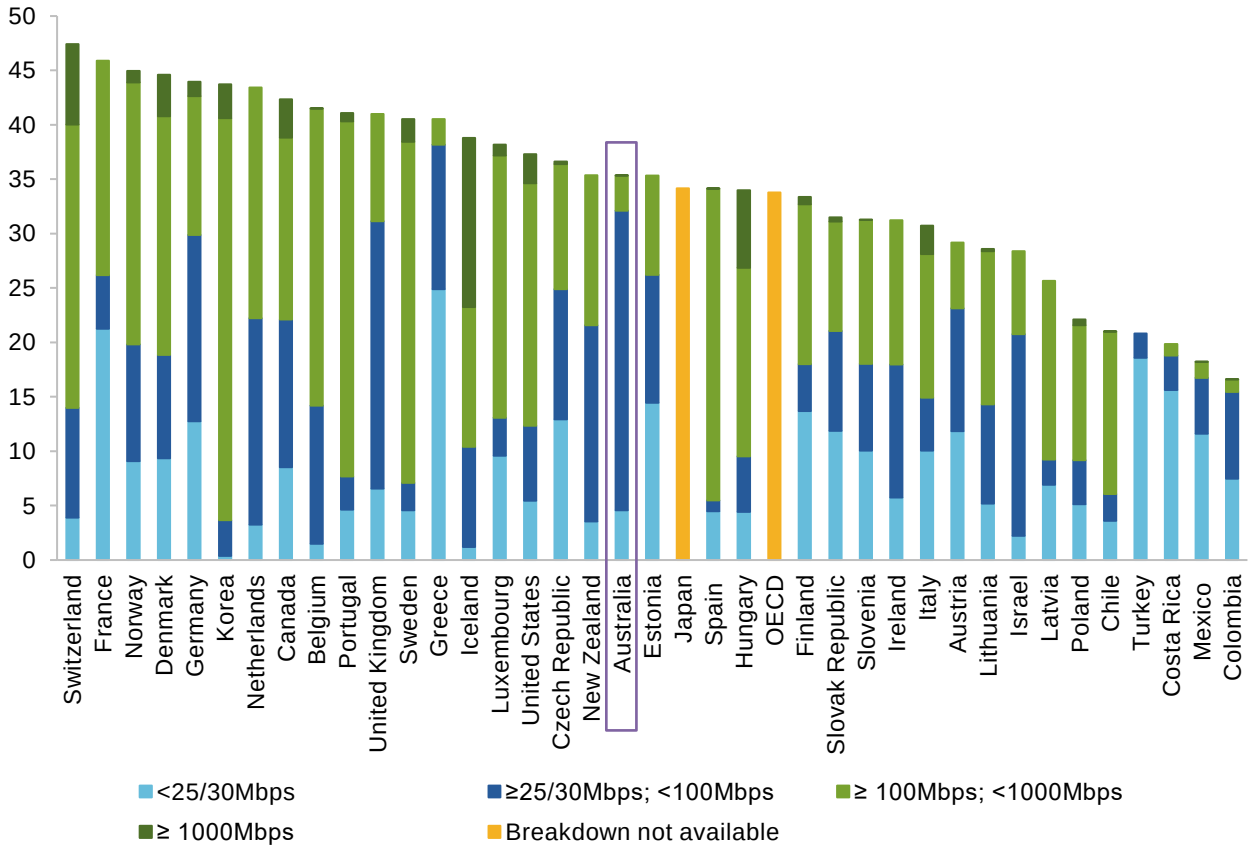
Source: OECD (2022b).

However, Australia's internet speeds are lower than many other OECD countries, particularly for fixed broadband connections. The majority of fixed broadband subscriptions in Australia are between 25/30 megabits per second (Mbps) and 100 Mbps (figure 1.9). Other countries — such as Switzerland, Korea and the United States — have a much higher proportion of fixed broadband subscriptions with speeds of 100 Mbps or higher. Moreover, speed test data shows that Australia's actual internet speeds are not globally

competitive. In the year to January 2022, Speedtest by Ookla reported that Australia's median mobile internet download speed was 68.35 Mbps (ranking 18th in the world) and the median fixed broadband download speed was 50.89 Mbps (ranking 61st) (Ookla Speedtest 2022).[4]

Figure 1.9 – Australia has many middling speed connections

Fixed broadband subscriptions per 100 inhabitants by download speed tiers, June 2021



Source: OECD (2022a).

Australia's large number of 25–100 Mbps subscriptions could reflect digital infrastructure (discussed in section 3.1) and broadband pricing, as many internet users may have a connection that could accommodate a faster subscription but choose to purchase a lower speed plan. Previous research has found that Australia ranks fourth out of 13 OECD countries on broadband affordability (measured using median price as a share of per capita income) for the 26–50 Mbps speed tier, but sixth for the 51–100 Mbps tier — below France, Japan, South Korea, Germany and the United States (Accenture 2021, p. 15). However, the report did not examine pricing and affordability for speeds higher than 100 Mbps.

Whether or not Australia's broadband speeds provide an adequate baseline of connectivity for businesses depends on what businesses need their internet connections for and what emerging technology this enables businesses to adopt, now and in the future. For example, speeds of greater than 100 Mbps increase the

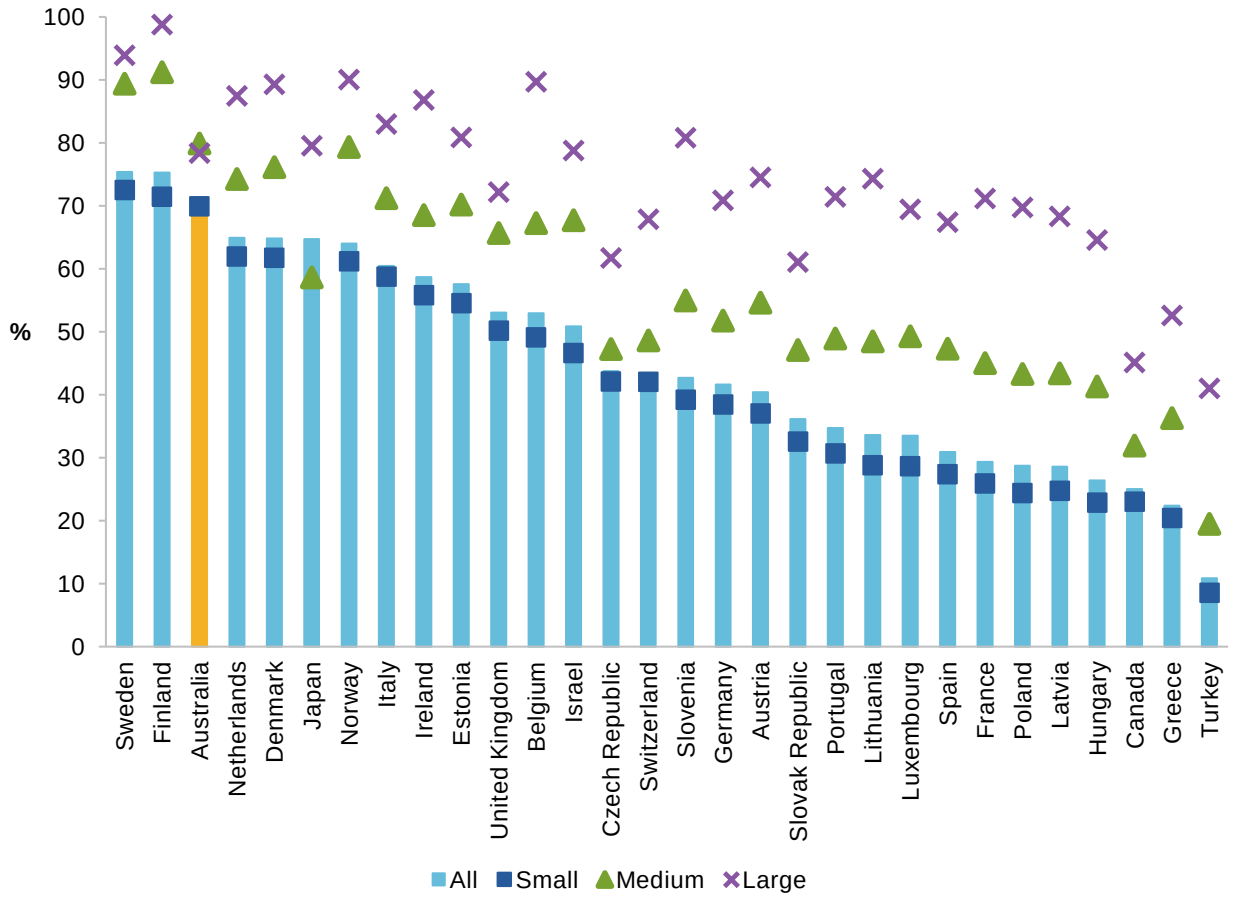
[4] Speed test rankings from an individual source must be interpreted with caution, because they are based on the selected sample of internet users that perform speed checks with that source (AlphaBeta 2019b). The OECD reports that Australia has consistently low fixed broadband download speeds across several different sources, including Ookla, M-Lab and Steam (OECD 2022a).

capacity of businesses to use cloud services and host multiple servers (Francom 2020), implying that lower speeds may constrain the uptake of these services. Internet speeds will also affect how many devices can be connected to a network (Antonelli 2022), suggesting that uptake of IoT devices may also be curtailed if the average speeds of Australian internet are insufficient.

Notwithstanding these relatively lower speeds — and perhaps in part driven by relatively high internet coverage — Australian businesses have higher rates of cloud technology adoption than many other countries. The share of businesses using cloud technology in Australia is third in the OECD, with 71% of businesses purchasing cloud computing services (figure 1.10). Evidence suggests that Australia's comparatively high uptake of cloud technology has persisted for some time, with earlier research finding that Australia had the second highest per-capita cloud computing expenditure in 2015, at US$371.50 (second only to Singapore, which had expenditure of US$539) (Gutierrez, Boukrami and Lumsden 2015).

Figure 1.10 – Australian businesses do relatively well on cloud adoption[a,b]

Share of businesses purchasing cloud computing services by firm size, 2021



a. Australian data refers to the fiscal year ending 30 June 2020 instead of 2021. **b.** For Israel and United Kingdom, data refer to 2020 instead of 2021. For Canada, Japan and Switzerland data refer to 2019 instead of 2021. For Japan, data refer to businesses with 100 or more employees instead of 10 or more; medium-sized enterprises have 100-299 employees and large ones 300 or more.

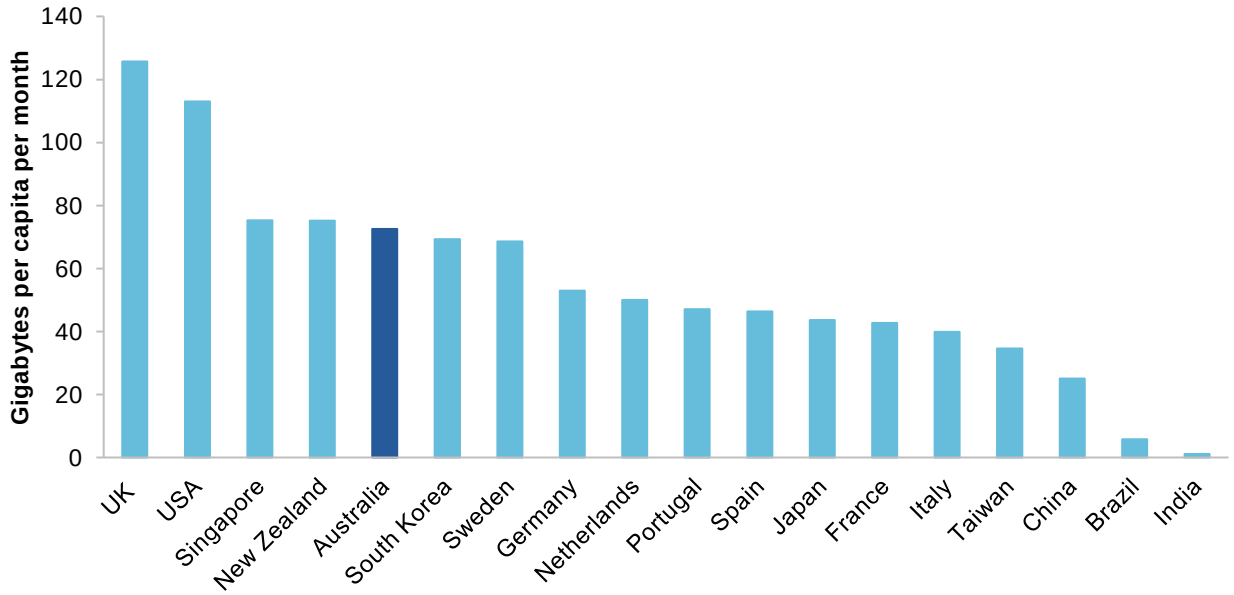
Source: OECD (2022a).

Data consumption is high but use of data-driven technologies is low

The production, sharing, analysis and use of data can significantly improve economic outcomes (as discussed in section 2.2) and Australia performs relatively well as both a data producer and consumer. For example, in 2019 the Harvard Business Review ranked Australia as 9th in the world on a list of 'new' data producers, based on our internet use and accessibility scores (Chakravorti, Bhalla and Chaturvedi 2019). Australia is also a comparatively large consumer of data, with per-capita download volumes similar to countries such as Singapore, New Zealand, South Korea and Sweden (figure 1.11).

Figure 1.11 – Australia's data download volumes are relatively high

Fixed broadband data consumption, 2019

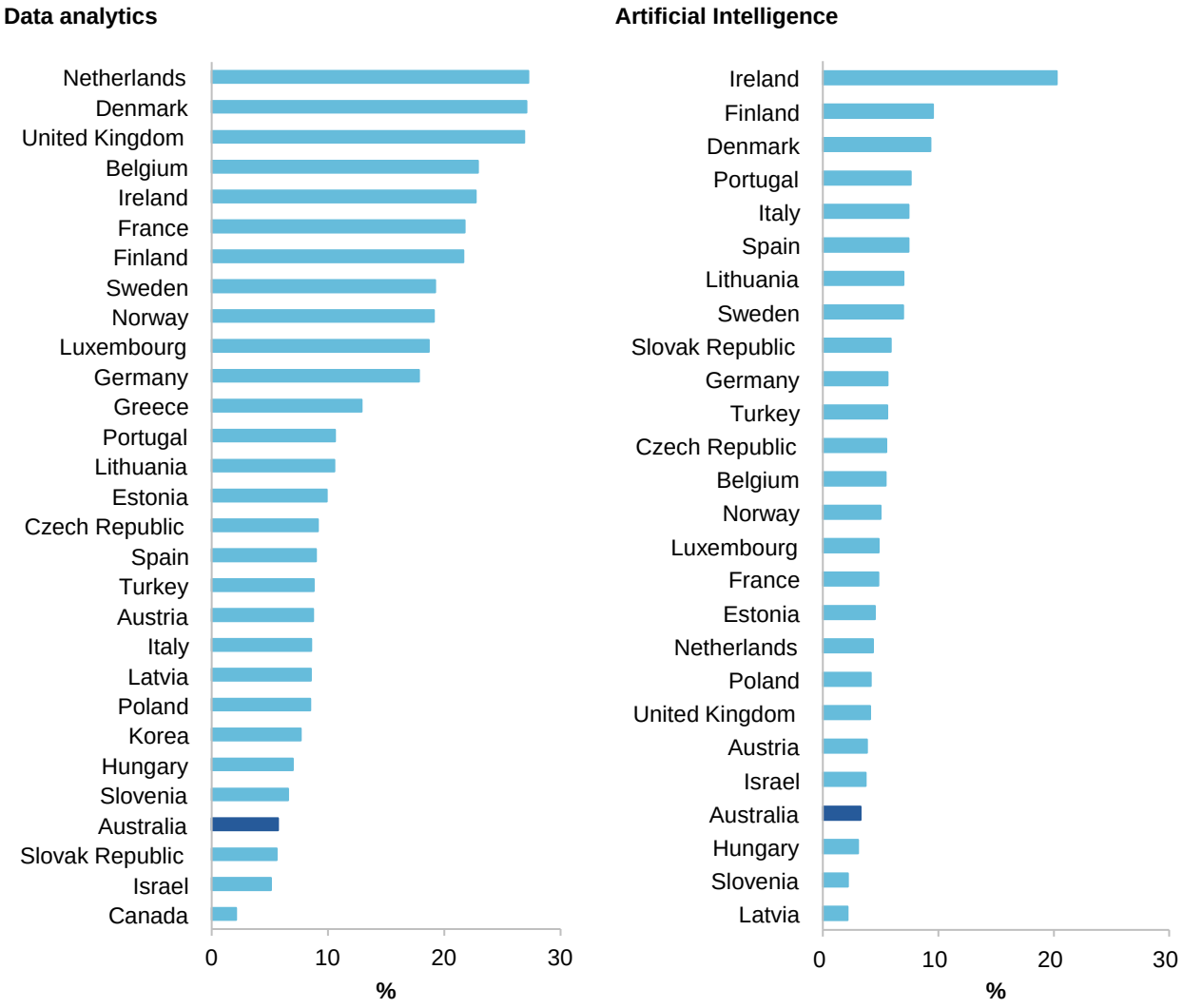


Source: Ofcom (2022).

These significant data volumes suggest that Australia has a lot of potential to leverage data-driven technologies, such as AI and data analytics (box 1.1), for productivity gains. However, adoption of these technologies is currently low compared with other countries. Only 6% of Australian businesses were using data analytics (such as working with big data or geospatial technology) in 2019-20 and an even lower share were using AI — in both cases, Australia's adoption is low compared with other countries in the OECD (figure 1.12). Some other studies have suggested that Australia performs relatively well in AI; for example, Zhang et al. (2021) ranked Australia at 8th in the world in 2020. However, this high ranking is partly due to Australia's performance in AI research (such as journal citations and publications), which does not necessarily translate to more use of AI by businesses.

Figure 1.12 – Australian businesses are trailing in use of data-driven technologies

Share of businesses who use data analytics, 2019[a], and artificial intelligence, 2020



a. While international data on data analytics use in 2019 has been sourced from the OECD, the share of Australian businesses using data analytics is from the ABS for 2019-20 (figure 1.4). The OECD's statistics do not include Australia in the cross-country comparison on use of data analytics.

Source: ABS (*Characteristics of Australian Business* 2019-20 financial year, cat. No. 8167.0), OECD (2022b, 2022a).

Finding 4.4
Australia trails behind other countries in more advanced uses of technology

Australia performs well compared with other developed economies on foundations such as internet connections and data volumes. But we trail in some more advanced indicators such as internet speeds and use of data-driven technologies.

2. Potential barriers to adopting new technologies and data

Key points

- **Although many businesses are adopting digital tools to improve their productivity, there are some barriers slowing the adoption of new uses of technology and data across the economy.**
- **The most common barriers to technology and data adoption identified by Australian businesses are inadequate internet, lack of skills, limited awareness and uncertainty about benefits, cost and legacy systems.**
  - Agriculture businesses are most likely to cite unsuitable internet speed and geographic location as barriers, suggesting poor digital connectivity in regional and remote areas could be limiting adoption.
  - High costs are more frequently identified as a barrier by medium and large businesses, which could reflect the costs associated with transitioning from legacy systems and established processes towards new technologies and ways of working.
- **More broadly, unique features of the digital and data environment could hinder adoption. For instance, without clear rules about access and rights, data is likely to be underutilised as potential users could be excluded. Businesses are also likely to underinvest in cyber security because the costs of cyber attacks to an individual business are often less than the costs of such attacks to society more broadly.**

2.1 Business-level barriers to digital and data uptake

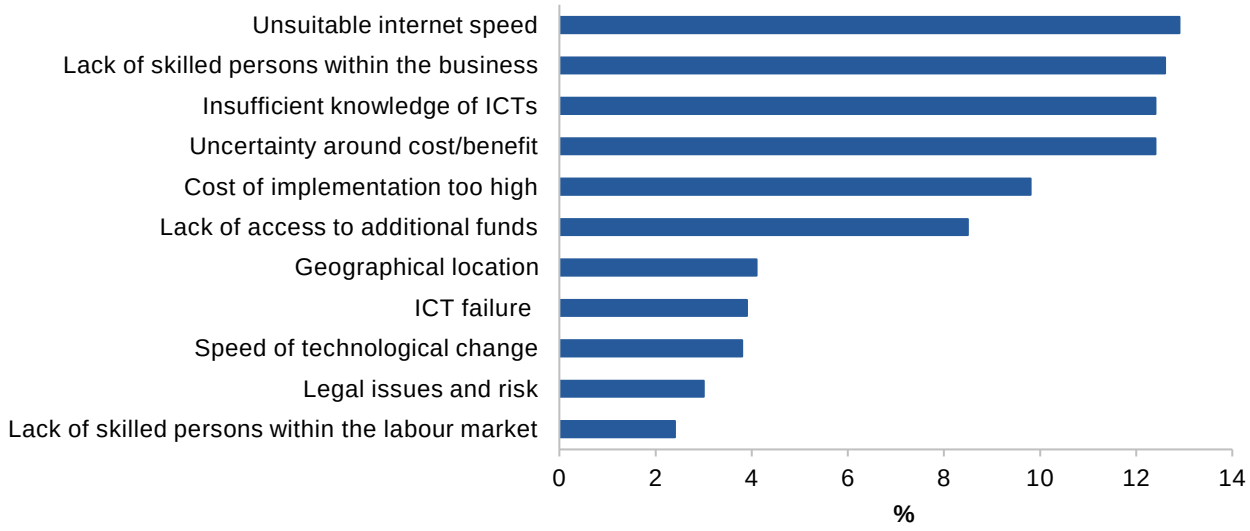
In deciding whether to adopt digital technology and new uses of data, Australian businesses weigh up the significant benefits (outlined in section 1.1) against the costs of adoption and barriers that may be preventing uptake. Businesses report that in 2019-20, the top factors that limited their use of technology were inadequate internet speeds, lack of skills and knowledge in the business, and cost or benefit uncertainties (figure 2.1). Various other studies of businesses in Australia and around the world have found similar barriers to adoption.

- Certified Practising Accountants Australia's survey of over 700 businesses in Australia, China, Hong Kong, Macau, Malaysia and Singapore found that the top technology adoption challenges are 'financial constraints', 'shortage of technology talent' and 'complex legacy systems' (CPA Australia 2021, p. 22).
- Deloitte Access Economics' survey of about 500 Australian small businesses reported that the main barrier to digital engagement is costs, followed by issues relating to awareness and decision making (for example, businesses believing that digital and data are not relevant to their business or simply not having thought about their use) (DAE 2019a, p. 11).

- Xero's research on behavioural barriers to adoption surveyed more than 4200 small businesses in Australia, New Zealand, Singapore, the United States, the United Kingdom and Canada, and found the top issues were resistance to change and uncertainty (Xero 2021a, p. 13).

Figure 2.1 – Internet speed and lack of skills are the biggest barriers to adoption

Share of businesses citing each factor as limiting their use of ICTs, 2019-20[a]



a. This chart uses weighted estimates as published by the ABS in its *Characteristics of Australian Business* 2019-20 publication.

Source: ABS (*Characteristics of Australian Busine*ss, 2019-20 financial year, Cat. no. 8167.0).

The specific nature of these barriers varies from business to business. Issues about cost, for instance, could relate to upfront costs of upgrading systems and processes, as well as ongoing costs related to new uses of technology and data. This financial equation is changing as many of these new applications are accessed via software-as-a-service models rather than through on-premise software and servers — TechnologyOne, which provides both types of products, estimates that 'moving to a SaaS approach can lower IT costs by up to 30%' (TechnologyOne 2019, p. 3).

However, businesses that are transitioning from legacy systems must also factor in the costs of changing processes and training staff to work with new digital tools. These represent additional sources of cost and uncertainty and can affect businesses of all sizes. Smaller businesses may not have the time or resources to navigate significant change; for example, Xero has observed that Australian small businesses are 'stuck in a "wait and see" mode with new technology – they're reasonably excited about its potential, but not so much so that they'll step into uncharted waters' (Xero 2021a, p. 26). Meanwhile, larger businesses may have more substantive legacy systems that need to be updated, and implementing significant changes to what could be long-established processes requires large amounts of time and investment (discussed below).

Lack of skills and talent can also manifest as a barrier in different ways across different businesses. In some cases, this relates to the specialist knowledge and capabilities of workers that need to use technology and data in their roles. Research by Gartner has found that talent availability inhibits technology adoption across a range of digital and data domains — including automation, security and digital workplaces — and that skills challenges have become more prominent since 2020 (Gartner 2021). Australian workers' digital and data-related skills are discussed in further detail in section 3.3.

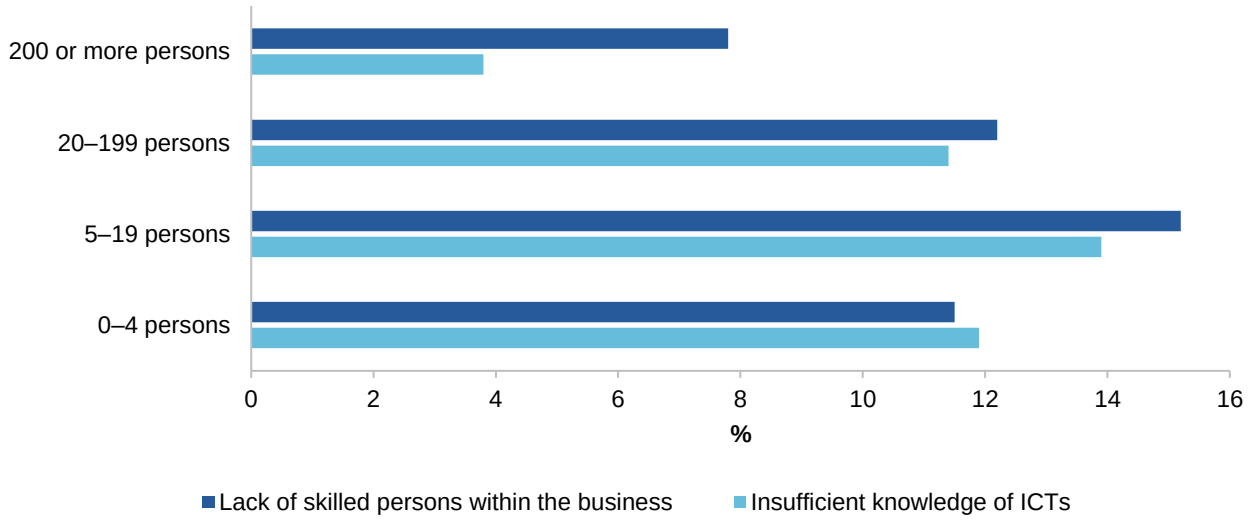
In other cases, adoption of innovative uses of technology and data is hindered by the capabilities of senior leadership. For example, a survey of 1300 executives in businesses from Australia, China, France, Germany, Japan, the United States and the United Kingdom found that 'while 81% of the executives agree that data skills are required to become a senior leader in their companies, 67% say they are not comfortable accessing or using data themselves' (Davenport and Mittal 2020). Limited skills could mean that senior leadership is unaware of the potential benefits of adopting digital and data tools, and as strategic decisions are often made at this senior level, this lack of relevant skills could slow business uptake.

The barriers that Australian businesses face in adopting technology and data vary depending on business characteristics. For example, in 2019-20 (ABS 2021a):

- unsuitable internet speed was a particular problem in the agriculture, forestry and fishing industry — 28% of agriculture businesses identified this as a barrier, almost double the rate of the next-highest industry (retail trade, 16%). In addition, 22% of agriculture businesses stated that geographic location limited their technology use, which was also double that of the next-highest industry (mining, 11%). As agriculture businesses primarily operate in regional and remote Australia, this indicates that internet connectivity and digital infrastructure could be a barrier to productivity-enhancing technology adoption in these locations
- high implementation costs were more likely to be identified as a factor limiting technology uptake by medium businesses (17% of businesses employing 20 to 199 persons) and large businesses (15% of businesses employing 200 or more persons), rather than small businesses. As discussed above, transitioning from legacy systems to new technologies can involve significant costs, and medium and large businesses are more likely to have established processes that are costly to change and therefore present larger barriers to adoption
- the most frequently cited skills barriers — lack of skilled persons in the business and insufficient knowledge of ICTs — were more likely to be identified as limiting factors by small and medium businesses, and particularly businesses employing 5 to 19 persons (figure 2.2).

Figure 2.2 – Small businesses are more likely than micro, medium and large businesses to face skills barriers to adoption

Share of businesses citing skills factors as limiting their use of ICTs by business size, 2019-20[a]



a. This chart uses weighted estimates as published by the ABS in its *Characteristics of Australian Business 2019-20* publication.

Source: ABS (*Characteristics of Australian Business,* 2019-20 financial year, Cat. no. 8167.0).

Finding 4.5
There are various barriers to business adoption of technology

Australian businesses report challenges to adopting digital and data tools that include: inadequate internet, lack of skills, limited awareness and uncertainty about benefits and costs, and legacy systems. Inadequate internet connectivity and speed are particular issues in the agriculture industry, while skills barriers are more likely to be identified by smaller businesses.

2.2 Broader limitations in the digital and data environment

Beyond the barriers to adoption experienced by individual businesses, there are broader issues that are unique to data and digital use that could limit uptake of productivity-enhancing technologies and processes. These include complexities in how data is created, used and shared; and the potential for underinvestment in cyber security to jeopardise the economic gains from greater use of technology and data.

Excessive exclusions to data use weakens its value

Improving data use benefits the economy through several channels

The near-endless possible uses of data means its potential value can vary between data users and applications, as well as over time. There have been some efforts to quantify the value of existing data based on the costs of producing that data.[5] Income- and market-based valuation approaches are also sometimes used, though in many cases the income streams attributable to a dataset are not easily identified or predicted, and few market prices are observed for data (Coyle and Manley 2022, pp. 8–9). The OECD observes that 'access to data alone does not generate value — rather, the value from data is derived in its use and after it has been collected, organised, and acted upon. …Therefore, the value of data is difficult to quantify, as data that is not valuable today may become so tomorrow' (Jouanjean et al. 2020, p. 13).

Deriving value from collecting, organising and acting upon data creates opportunities for productivity gains. The Commission's 2017 *Data Availability and Use* inquiry detailed the breadth of potential benefits associated with more access and use of data, as they relate to individuals, businesses and society (PC 2017a, ch. 2). The channels that are most relevant for enhancing productivity include:

- more competition — data allows consumers to make better comparisons on the price and quality of different goods and services, particularly for complex products such as in financial services or healthcare. This enables consumers to make more informed decisions about the products they purchase, providing greater impetus for businesses (and governments) to compete either on price or product features

[5] For example, Statistics Canada has estimated the value of data based on 'the labour costs incurred in their production plus associated non-direct labour and other costs, such as the costs of the associated human resource management and financial control, electricity, building maintenance and telecommunications services' (Statistics Canada 2019). The ABS has applied this sum-of-costs approach to Australia, finding that 'valuing data as an asset within the national accounts may increase GDP in the order of 2% and would have little impact on the value of capital stock (dependent on the asset life chosen)' (Smedes, Nguyen and Tenburren 2022, p. 10).

- fuelling innovation — businesses and governments can use data as the basis for new goods and services or incremental improvements to existing ones, as it furthers their understanding of what does and does not work. The data may also be a direct input to the new or improved product, such as when the product relies on an algorithm for part of its decision making
- improving allocative efficiency — data enables resources to be allocated more efficiently by both the private and public sectors. At a micro level, individual inputs (such as energy or worker time) can be monitored and shifted to higher-value uses as required. From a macro perspective, data can be used to identify parts of a system (such as the hospital system) that are over or under capacity, and resources can then be directed accordingly
- targeting government interventions — data can enable governments to better target their interventions in the economy to achieve social and community outcomes, such as public health and safety, income support for people in hardship or environmental improvements.

While these economic opportunities relate to data itself regardless of whether or not the data is digitised, in practice many benefits are realised at scale when digital technologies are used to collect and analyse data, due to the significant lowering of transaction costs (section 1.1).

The ability for data to be used for productivity gains can vary over time. For example, in some cases the value that can be created from using data to improve a product diminishes as more data is collected and analysed — the information contained in the purchases of the first 1000 customers is likely to be more useful than data from the 1 000 001st to 1 001 000th customers a year later. Data can also become obsolete over time; for instance, data from a couple of months ago has lower value for informing resource allocation now, compared with making similar decisions at the time the data was collected. Alternatively, new digital technologies may open up value from previously underutilised datasets.

Moreover, the economic benefits associated with the above opportunities sometimes stem from interdependencies in how data is valued and used by different stakeholders. For example, a consumer gets value from data on their previous purchase decisions because it can help to inform their preferences when buying related goods and services in the future. Because of this, businesses selling similar products can make use of this preference data to improve their offerings and therefore their competitiveness relative to other sellers. These interdependencies mean that maximising the productivity gains associated with using data may require data linkage between multiple sources or stakeholders, as well as analytic capabilities to extract useful insights (OECD 2015, p. 186).

Making data available in private and public contexts

Given the potential economic benefits, making data widely available for businesses and governments to use could generate significant productivity gains. However, as discussed in section 1.1, external parties can be excluded from accessing and using data, even though its use in the production process is non-rivalrous. While this excludability provides a mechanism for incentivising data production and collection, it also prevents others from using the data to create new economic value. In this context, restrictions placed on data access are conceptually similar to intellectual property, where there is also a trade-off between broader access to something and its exclusive use, with this balance often struck by granting content creators

exclusive intellectual property rights for a limited time.[6] However, such time-based, temporary rights over data generally have not been developed in Australia or elsewhere.

A private business that controls data may find it profit maximising to exclude other parties from that data. For example, it has been claimed that control of customer data enables digital platforms to create barriers to entry by rival businesses and to limit competition, particularly in search and advertising technology services (ACCC 2022d, pp. 166–167). Nonetheless, private organisations may share data on their own accord if there are mutual benefits and regulatory requirements such as privacy laws and commercial contract conditions are adhered to. Research by the European Commission noted that where there are gains for multiple private parties, even if there is no overarching framework requiring data sharing, 'bargaining in data markets produces a de facto ownership or residual rights allocation, both in commercial [business-to-business] and in personal [business-to-consumer] data settings' (Duch-Brown, Martens and Mueller-Langer 2017, p. 46). For example, advanced manufacturing businesses have generated efficiency improvements through private agreements to share real-time engineering data with their suppliers, which enables faster product design, more flexible operations and better cost management (ODI 2020, p. 2).

But as the non-rivalrous nature of data means that it can be very widely used across the economy, it is likely that these private market-based solutions would not result in a socially optimal allocation of data. The OECD has observed that 'greater social value is created with greater use of common resources [as] in the case of non-rivalrous goods such as data. This is the strongest rationale for policy makers to promote access to data' (OECD 2015, p. 38). There are various mechanisms that governments can use to reduce the capacity of private entities to undesirably exclude others from accessing data, such as by implementing a framework that establishes rights over data and requires that data is shared if requested by someone with a right over it. An example of this is Australia's Consumer Data Right, discussed in further detail in section 3.2.

Because excludability sometimes provides the incentive for private organisations to invest in collecting, cleaning and storing data for their own uses (section 1.1), government requirements compelling these organisations to share their data could erode some of the private economic benefits that they realise from their investment and/or reduce the quality of data available. In some cases, individuals may be less accepting of making their data available to a private organisation if they know that the organisation is compelled, in turn, to share that data with a third party. Efforts to increase data sharing to enable more or higher value uses of non-rivalrous data must therefore be balanced against the risks of disincentivising future data production (as well as taking into consideration privacy and data security concerns). Governments also face challenges in specifying the optimal level of access 'because it is difficult to know ex-ante what the social welfare maximizing arrangement would be, [so] regulators may have little guidance for an intervention' (Duch-Brown, Martens and Mueller-Langer 2017, p. 47).

The socially optimal amount of data availability varies based on the private or public nature of the benefits and costs associated with its use. It can also depend on whether private or public sector entities are involved in collecting and holding the data. Data can be produced purely by the public sector, purely by the private sector or somewhere in between these two ends of the spectrum (for example, jointly produced by public and private entities or collected and held by private businesses but funded by government). The role of government varies in these scenarios — section 3.2 explores different ways that government can support data sharing and use in different contexts.

[6] The Commission previously examined intellectual property rights in its 2016 *Intellectual Property Arrangements* inquiry. In highlighting the trade-off between production and use, the inquiry stated that intellectual property rights should aim to provide 'appropriate incentives for innovation, investment and the production of creative works while ensuring it does not unreasonably impede further innovation, competition, investment and access to goods and services' (PC 2016, p. 6).

Finding 4.6
Data sharing enables productivity growth but can reduce incentives to invest in data

More access to and better use of data enables productivity growth by increasing competition, innovation and allocative efficiency. But efforts to increase data sharing could discourage quality future data production if they erode the economic benefits that private organisations can realise from investing in data collection and analysis. As such, increased data access must be balanced alongside incentives for the ongoing collection and maintenance of quality data, as well as privacy and data security concerns.

Businesses are likely to be underinvesting in cyber security

Poor cyber security jeopardises economic gains

As the use of technologies and data has spread throughout the Australian economy, so too have the risks that attacks on the digital systems and networks that underpin these activities can directly affect economic prosperity. There are multiple sources of risks and points of vulnerability; for example, unprotected software and hardware and human error.

The number of cyber crime incidents is growing in Australia, with cyber crime reports to the Australian Cyber Security Centre (ACSC) increasing to 76 000 incidents in 2021-22, up 13% on the previous financial year (ACSC 2022a, p. 11). In 2021-22, the most common type of cyber crime reported was fraud, representing 27% of all reports (figure 2.3), while many of the shopping and online banking incidents were scams involving loss of finances or personal information. Online scams not only harm consumers but can significantly reduce businesses' confidence in digitising or adopting new technologies, with the ACCC observing that it can be very difficult to repair the damage inflicted by scams after they have occurred (ACCC 2021e, p. 2). About 450 ransomware attacks were reported in 2021-22; while low in number, the ACSC noted that it is likely ransomware is significantly underreported, 'especially by victims who choose to pay a ransom' (ACSC 2022a, p. 47).

Most cyber security incidents are self reported in Australia, so the true magnitude of cyber crime is unknown. However, international analysis on the extent of cyber breaches undertaken by global cyber security software providers indicates that Australian businesses receive a large share of cyber attacks. For example, Australia was the third-most targeted country based on ransomware intrusion volumes in 2021, behind the United States and Italy (Accenture 2022, p. 5), and a 2020 survey found that Australia had the highest percentage of firms reporting a ransomware attack in the previous 12 months (CyberEdge 2021, p. 23).

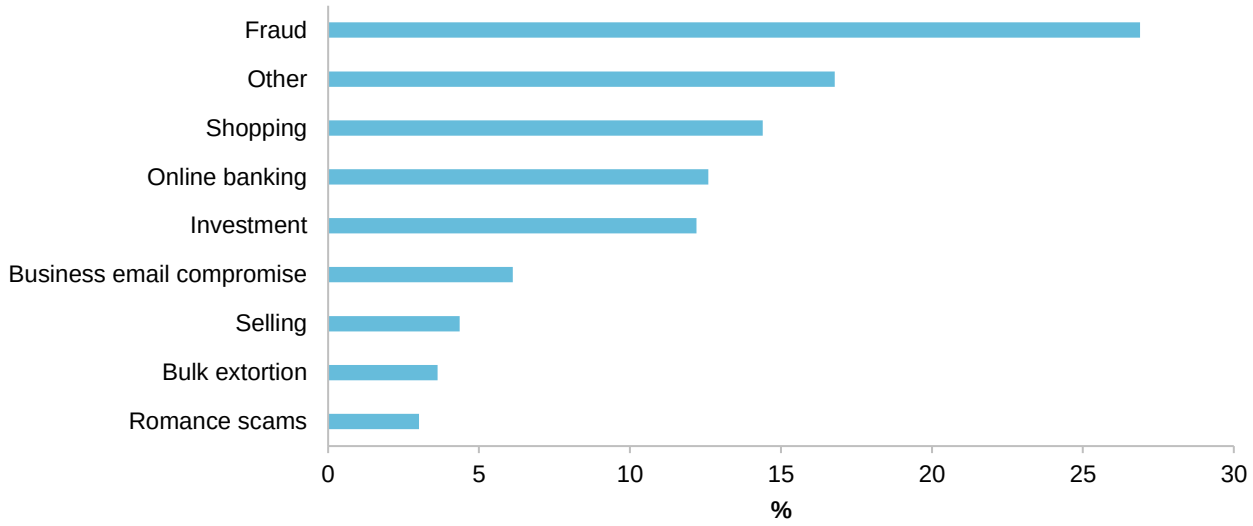
Cyber security is an important pre-condition for effective use of digital technology and data, and poor security practices can limit productivity and economic gains in several ways.[7] First, concerns about security risks can prevent uptake of digital tools and data analysis. For instance, concerns about security and lack of trust in service providers are a barrier to cloud adoption (Alismaili et al. 2020), with 10% of Australian businesses citing security concerns as a reason for not adopting cloud technology (ABS 2021a). Conversely, providing

[7] The Australian Government differentiates between cyber security — which involves 'protecting data, information, devices and networks from malicious actors' — and online safety, or protection from 'harmful content and behaviours such as cyber bulling, image-based abuse and illegal and harmful online content' (Home Affairs 2020a, p. 35). This report focuses on cyber security rather than online safety, as it is the main factor that could affect productivity.

assurance and confidence in digital and data systems and processes, and minimising the risks involved, can support adoption.[8]

Figure 2.3 – Fraud is the most common cyber crime reported in Australia

Cyber crime reports made to the ACSC by crime type, 2021-22[a]



a. The 'other' category includes crimes such as harassment and malware.

Source: ACSC (2022a, p. 23).

Second, cyber security incidents can also have significant economic consequences in terms of lost output or productivity. In Australia, the ACSC stated that self-reported losses from cyber crime totalled more than A$33 billion in 2020-21 (ACSC 2021a, p. 17) and worldwide, the Centre for Strategic and International Studies estimated that in 2020 the cost of cyber crime to the global economy was US$945 billion (Smith, Lostri and Lewis 2020, p. 3). The impact on an individual business can be significant; for example:

- the average cost of a data breach to Australian businesses was estimated to be US$2.8 million in 2021, when taking into account the direct and indirect costs of 'detection and escalation, notification, post breach response and lost business' (IBM 2021, p. 9)
- 60% of all targeted cyber attacks strike small and medium businesses, and the average time to resolve an attack is 23 days — though this more than doubles to 51 days if the attack stemmed from a malicious insider, employee or contractor (Australian Government 2015)
- two-thirds of small and medium businesses would have to shut down for at least a day, and potentially go out of business, if they were hit with a data breach (Forrest 2017).

While security expenditure is increasing, not all risks and costs are considered

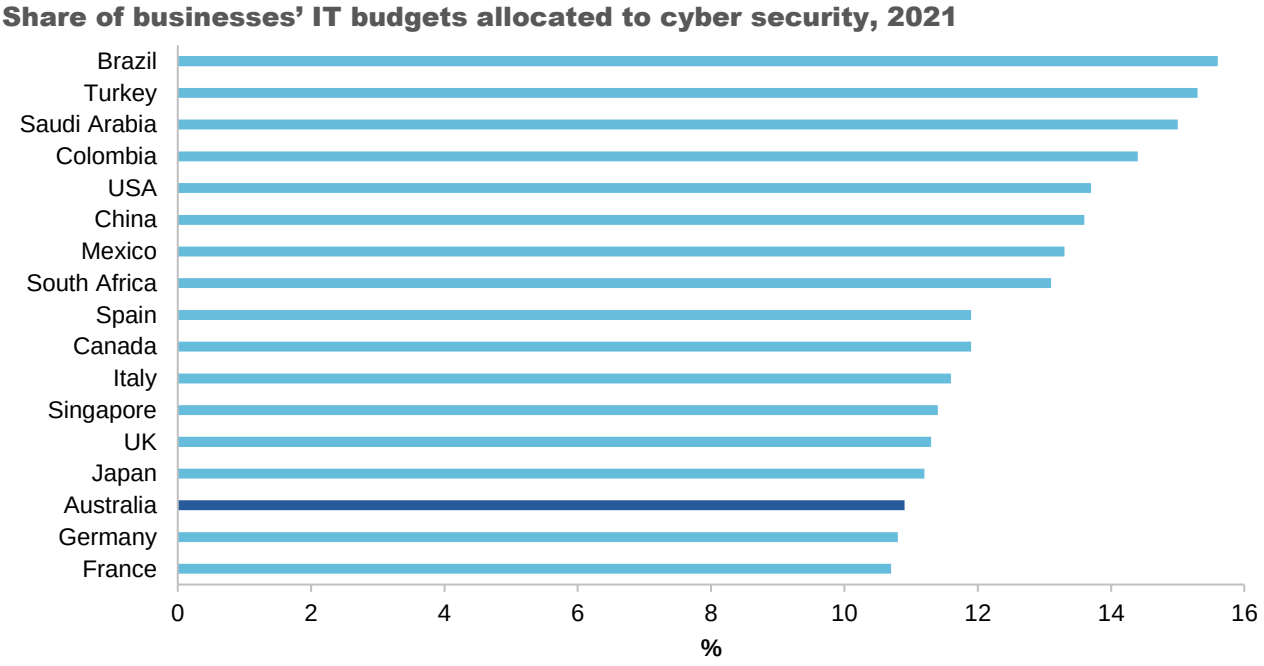
Australians are already increasingly investing in cyber security to protect themselves from the costs of cyber attacks and breaches. AustCyber estimates that Australia's total cyber security expenditure was $5.6 billion in 2020, having increased at an average annual rate of 9% between 2017 and 2020 (AustCyber 2020, p. 8). Providers of cyber security products and services earn about 30% of their revenue from sales to government customers (including in the healthcare, social care, education and defence sectors) and up to 25% from financial

[8] But there is also often a trade-off between security of data and access to (and hence efficient use of) data, implying that there is an optimal level of insecurity (Moore 2010, p. 106).

services customers (AustCyber 2020, p. 19). However, this only reflects expenditure on external cyber security products and services — businesses in some sectors, such as technology and financial services, are reportedly building internal cyber capabilities rather than purchasing from external providers (AustCyber 2020, p. 19).

International estimates suggest that Australian businesses have a comparatively low share of IT expenditure dedicated towards cyber security — about 11% in 2021 (figure 2.4), down from 13% in 2020 (CyberEdge 2021, p. 29). Moreover, expenditure on cyber security in itself is not sufficient to mitigate risks, as companies also need to ensure that their security products are integrated into broader business practices, capabilities and culture (Braue 2022).

Figure 2.4 –Australian businesses' IT expenditure allocated to cyber security is comparatively low



Source: CyberEdge (2022, p. 32).

As many of the benefits from using digital technologies stem from greater connectivity between stakeholders and systems, the costs of a security incident affecting one person or business can have negative consequences for a much larger group. This negative externality can have significant consequences: 'information systems are prone to fail when the person or firm responsible for protecting the system is not the one who suffers when it fails. Unfortunately, in many circumstances online risks are allocated poorly' (Moore 2010, p. 105). For example, the total cost of a security breach to a business that collects and holds customer data electronically is higher than the cost incurred by the business itself, as all of that business's customers would be affected and the negative impacts could also extend to compromising confidence in other businesses in similar industries. The business would underinvest in cyber security if it fails to internalise these wider costs.

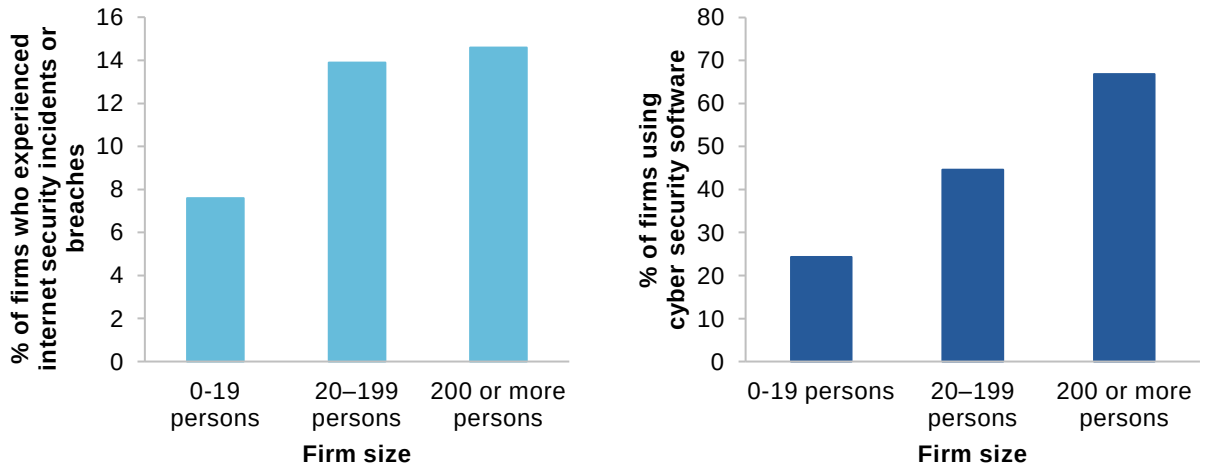
This issue is compounded by interdependencies in the use of digital and data tools, and information asymmetries when the users of these tools are relatively uninformed about potential security risks. Cyber criminals can exploit links between computer networks and systems to attack a wide range of users — for example, by targeting digital services providers to spread malware through software updates issued to their customers, as in 2017's NotPetya attack and 2021's SolarWinds attack (Huang, Pearlson and Madnick 2021). But it can be challenging to ascertain the extent of cyber security risks: individuals and

businesses may have difficulty verifying a software vendor's security performance, making them reluctant to incur additional costs for increased security with uncertain benefits (Kox and Straathof 2014, pp. 2–3). And where the reporting of security incidents is voluntary, most stakeholders have an incentive to underreport cyber attacks to avoid drawing attention to vulnerabilities and reduce reputational risks.

Businesses of different sizes have different experiences with cyber security risks and investments. The ABS's Business Characteristics Survey reported that in 2019-20, smaller businesses were comparatively less likely to experience (or at least report) a cyber breach or incident, whereas medium and large businesses were almost twice as likely to report that they were attacked (figure 2.5, left chart). While large businesses were correspondingly more likely to be using cyber security software (reported by two-thirds of large businesses), a smaller share of medium-sized firms (45%) used security software (figure 2.5, right chart), in spite of being almost as likely to experience an attack.

Figure 2.5 – Cyber threat and security levels vary by business size

Share of businesses experiencing incidents and using security software by business size, 2019-20[a]



a. This chart uses weighted estimates as published by the ABS in its *Characteristics of Australian Business 2019-20* publication.

Source: ABS (*Characteristics of Australian Business,* 2019-20 financial year, Cat. no. 8167.0).

Other studies have also found that small and medium enterprises (SMEs) have less mature cyber security practices, attributable to issues such as ad-hoc cyber budgets, poor preparation for incident response and a lack of understanding of technical security terms (Andal et al. 2022; Cynch Security et al. 2021). According to the Australian Chamber of Commerce and Industry, 'it is becoming increasingly important for SMEs in particular to look to the adoption and successful implementation of digital technologies within a trusted ecosystem, secured by design that is both robust and resilient' (ACCI, sub. 47, p. 25).

The negative externalities and information asymmetries associated with cyber risks and incidents provide the rationale for government policy on technology and data security, particularly in parts of the system that have many connections to other individuals and businesses, given the interdependencies described above. This is discussed in further detail in section 3.4.

Finding 4.7
Businesses can underinvest in cyber security protections

Cyber security attacks are costly to respond to and recover from, and security concerns can deter uptake of digital and data tools. Businesses that do not account for all of these costs to themselves and others are likely to underinvest in their cyber security. Small and medium businesses are less likely to have mature cyber security practices than large businesses.

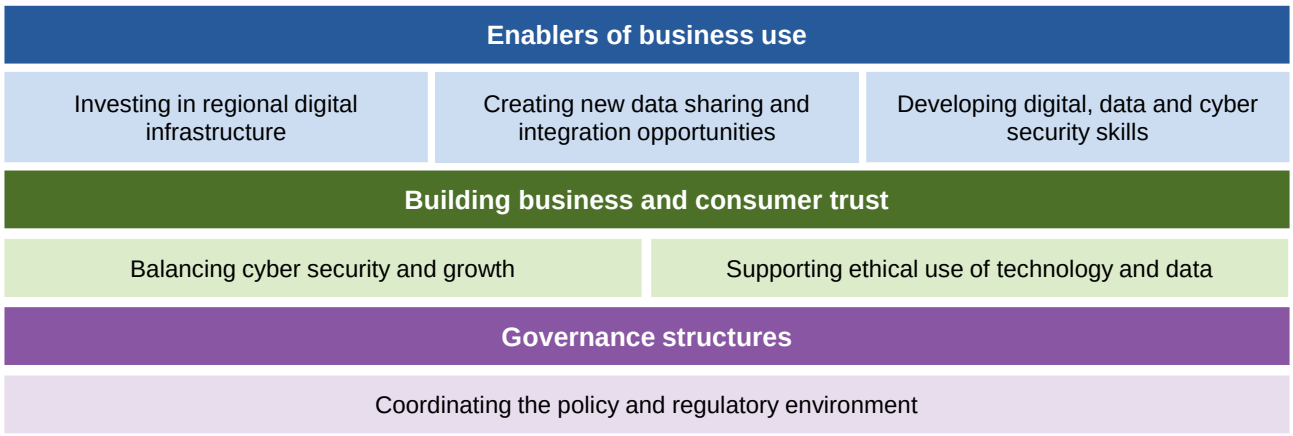
3. Targeting government investments and policy priorities

Key points

- **Technology change and increasing private sector provision of digital infrastructure have led to more options for regional and remote Australians to connect to the internet. Infrastructure funding arrangements that currently involve government decisions about technology type and location could be made more competitive and transparent. Competitive tendering could be a more efficient way to deliver the government's Universal Service Guarantee, subject to market feasibility.**
- **Data collected by providers of government-funded services is often not shared. More data sharing and interoperability in sectors such as health, education, aged care and childcare would improve services for consumers and system-level policy decisions. My Health Record could provide the foundation for this in the health sector with some further government efforts around data sharing obligations, software compatibility, security and de-identification. More broadly, the government can also facilitate more data sharing and use by extending the *Data Availability and Transparency Act 2022* (Cth) to allow government data sharing with the private sector, and expanding access to the Digital Identity.**
- **Meeting Australia's digital and data skills needs is an important enabler of future productivity growth. Industry certifications and short courses provide upskilling and reskilling options for workers to develop digital and data capabilities. Migration policy could better reflect employer demand for emerging skills.**
- **Secure use of technology and data is essential for maintaining business and consumer trust, and ensuring lack of trust does not become a barrier to adoption. More information is required to understand whether the government's regulation of high-risk critical infrastructure sectors has led to unintended economic consequences, such as higher costs or lower investment. Streamlining cyber security incident reporting via a single interface would reduce the administrative burden on businesses.**
- **Ethical use of technology and data — particularly via artificial intelligence — is an emerging focus area that is also required to build trust. While there is broad agreement on good ethical principles, translating these into action is challenging, and more information is required to determine whether government has a role to play. Regulation (such as privacy regulation) should be targeted to high-risk areas and balance legal and economic concerns to not unduly inhibit productivity growth.**
- **More coordination between digital, data and cyber security policy and regulatory agencies, and more engagement between agencies and industry, would reduce overlap and inconsistency and lower uncertainty for businesses.**

Government investments and policies provide the foundations that enable businesses to harness emerging digital technologies and uses of data, including by setting appropriate incentive frameworks and access rights, and addressing gaps where market provision is insufficient. The government can also support by building trust in these technologies and data uses among both businesses and consumers. Underpinning these initiatives, adaptable and coordinated governance structures are required to maximise the potential uses of digital technology and data, and minimise duplication and unnecessary burdens. This chapter explores six areas where the government could act to improve these foundations and support digital, data and cyber security activity in the Australian economy (figure 3.1).

Figure 3.1 – Potential areas for governments to improve Australia's digital, data and cyber security foundations



The Australian Government has already implemented a range of investments, policies and strategies relating to digital, data and cyber security. These are brought together in an overarching framework in the government's *Digital Economy Strategy 2030*, which seeks to establish Australia as a leading digital economy and society by 2030. The strategy has three pillars: 'building the foundations to grow the digital economy', 'building capability in emerging technologies' and 'setting Digital Growth Priorities to lift our ambition' (PMC 2021c, p. 3).

Given the significant government activity that is already underway in this space, the Commission has focused its discussion and policy recommendations in this chapter to areas where further action would be beneficial. Existing government initiatives are summarised, where relevant, as context to the analysis.

3.1 Investing in regional digital infrastructure

Ensuring that digital infrastructure, such as broadband and mobile networks, is fit for purpose is vital to underpin continued economic growth as technology advances. Australian businesses need this infrastructure to make best use of productivity-enhancing digital and data tools, and individuals require reliable connectivity to participate in work and society — including accessing essential services such as health, education and welfare support — in an increasingly digitised world. This is reflected in the government's Universal Service Guarantee for broadband connectivity, discussed in more detail later in this section.

Australia's population and economic activity is geographically dispersed across its large land mass. While much of it is clustered around capital cities, regional Australia accounts for about 40% of national economic output and employs about one third of Australia's workforce (RAI 2016, p. 4). More recently, the Commission observed that there has been some population movement from Australia's cities to regional areas since the

COVID-19 pandemic led to increased working from home. Although the number of people moving was small as a share of city populations, because regional areas have much smaller populations, the effects on local economies are likely to be more substantial. A population shift towards regional areas would increase demand for housing and infrastructure, such as telecommunications (PC 2021c, p. 71).

Adequate digital infrastructure is therefore required in both metropolitan areas and regional and remote Australia. But low-quality connectivity outside of Australia's cities is an ongoing issue (Internet Australia 2021). The Australian Government's 2021 *Regional Telecommunications Review* referred to the 'patchwork quilt' of connectivity in regional areas and noted that 'local councils and other regional stakeholders are increasingly expected to facilitate telecommunications service delivery, but are not appropriately resourced to identify connectivity needs and support the deployment of suitable solutions' (RTIR Committee 2021, p. 4). The Australian Local Government Association has noted that 'some regional and remote areas still lack access to reliable connectivity and pay a higher cost for services compared with their metropolitan counterparts' (ALGA, sub. 61, p. 5). Moreover, the Australian Digital Inclusion Index, which has run since 2014, shows an enduring disparity in internet access and speeds between regional and metropolitan areas (Thomas et al. 2021).

Infrastructure Australia reports that 23 of Australia's 48 regions have broadband and mobile connectivity infrastructure gaps under the Regional Infrastructure Gap Prioritisation Framework (figure 3.2). These are areas where broadband and mobile infrastructure 'does not ensure user, business and industry needs are met. The impacts of this gap are wide-ranging, with some remote communities suffering from social exclusion as a result of limited or non-existent telecommunications infrastructure' (IA 2022b, p. 41). For example, in the remote NSW town of Wilcannia, most residents access the internet through mobile connections but coverage 'is patchy and unreliable, congested in peak periods and has low penetration inside buildings… This is further exacerbated by Wilcannia's remoteness' (Featherstone, Ormond-Parker and Holcombe-James 2022, p. 6). As a result, residents have difficulties accessing services such as home schooling, entertainment streaming, telehealth consultations, online banking and work-related video calls. Better connectivity also enables essential services in remote communities to be linked together at lower cost — for example, by connecting schools, healthcare providers (including Aboriginal Community Controlled Health Organisations) and employment support (such as Centrelink services) so that they can deliver higher-quality services to local residents.

Improving regional digital infrastructure could lead to significant economic benefits and productivity gains. For instance, as discussed in section 2.1, unsuitable internet speeds and geographic location were particular barriers to technology adoption among agriculture, forestry and fishing businesses — which typically operate in regional and remote Australia. The Bureau of Communications, Arts and Regional Research estimated that:

> … the additional economic benefit from broadband-supported technology could be between $3.0 and $10.6 billion per year (in 2017–18 dollars) for the agricultural sector by 2029–30, which represents an additional boost to economic activity in agriculture of between 4.7 to 16.9 per cent by 2030. (BCARR 2021, p. 5)

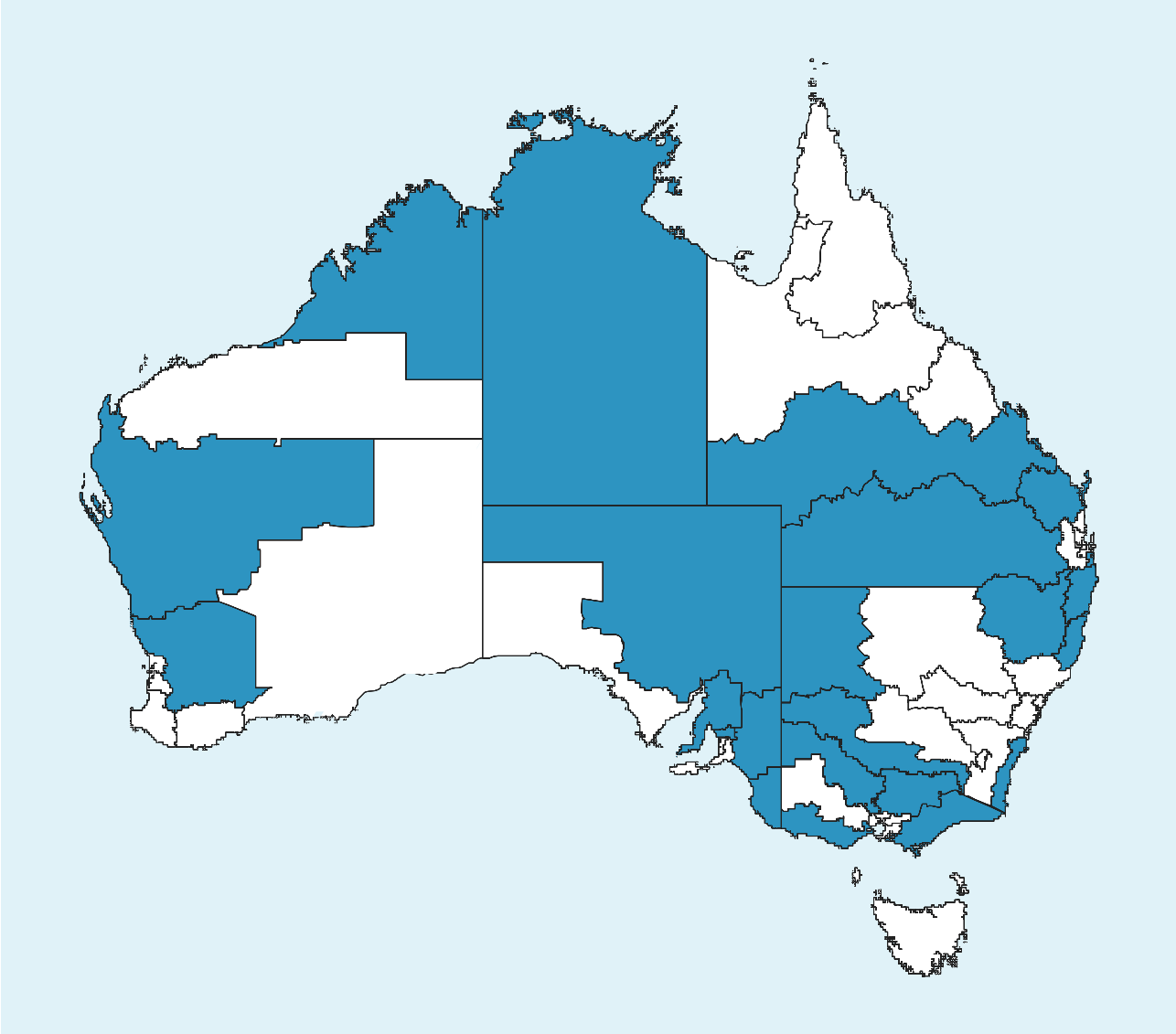
This includes through applications such as whole of farm connectivity solutions for crop and livestock production, which covers large areas, and using sensors to improve the allocation of water and other resources. Stylised whole-of-economy modelling undertaken by the Commission for this inquiry found that potential productivity improvements arising from improved regional digital infrastructure (leading to increased technology uptake in the agriculture and mining industries) would lead to increased real GDP, gross national income and wages (appendix B). Moreover, in addition to the social inclusion benefits discussed above, better access to digitally enabled health and education services in regional and remote areas could also

have economic dividends, such as increased workforce productivity and more efficient government expenditure on service delivery in these locations.

Regional digital infrastructure investment can be undertaken by both governments and private entities. The role for publicly funded investments should be limited to areas where the private sector is unwilling or unable to invest, so that governments avoid crowding out private sector investments that would otherwise have occurred.

Figure 3.2 – Almost half of Australia's regions have digital infrastructure gaps

Regions with broadband and mobile connectivity infrastructure gaps, 2022[a]



a. Blue shaded areas represent regions that Infrastructure Australia has identified as having broadband and mobile connectivity infrastructure gaps, defined as areas where the available infrastructure 'does not ensure user, business and industry needs are met. The impacts of this gap are wide-ranging, with some remote communities suffering from social exclusion as a result of limited or non-existent telecommunications infrastructure' (IA 2022b, p. 41).

Source: Infrastructure Australia (2022b, 2022c).

Finding 4.8
Inadequate internet in regional areas limits productivity gains and lowers social inclusion

Some regional and remote communities have poor internet connectivity, which can limit the ability of local industries to adopt productivity-enhancing technologies and reduce employment opportunities for local residents (if they are unable to work from home). Inadequate and unreliable connectivity also contributes to social exclusion, as residents are less able to access essential services (such as health, education and welfare support) in an increasingly digitised world.

The diverse technology and sectoral mix of investment

The evolution of digital infrastructure means that there are various ways that businesses and individuals can connect to the internet.

- Fixed broadband involves broadband services being delivered to a fixed location, and includes fixed line connections and fixed wireless connections. Fixed line involves running physical cable to a location. NBN services have a number of different fixed line connection types (such as fibre to the premises and fibre to the node), which have different ratios of fibre optic cable to copper cable, with more fibre being more expensive but resulting in a better connection. Fixed wireless connections use wireless receivers to connect a particular location, rather than using the mobile network.
- Mobile broadband connects users to the internet over the mobile network, requiring mobile base stations in the vicinity and access to radio frequency spectrum[9] to provide the network.
- Satellite technology connects the user via a satellite network, which has historically been a more expensive option than fixed and mobile services.

Different types of connections will be more or less appropriate depending on the location because of the infrastructure required. Fixed broadband services typically provide reliable internet, but the need for a physical connection and the lack of geographic flexibility mean that for some locations, mobile broadband will be more suitable. However, the reliance of mobile services on base stations can lead to intermittent internet service in mobile black spots. While satellite connections have been used primarily by very remote consumers, cost reductions with technology improvements and increased demand for business and household connectivity have increased satellite connections in less remote parts of Australia (primarily southern New South Wales and Victoria) over the past year (Fogg 2022).

The suitability of all connection types can change over time as technology progresses. For example, much of Australians' internet usage currently occurs through fixed broadband, but other types of connections may become more prominent in the future. The Bureau of Communications and Arts Research (now the Bureau of Communications, Arts and Regional Research) has observed that 'the bulk of data downloaded is through

[9] The Australian Government (specifically, the Minister for Communications) provides high-level policy guidance on Australia's spectrum resources, with the Australian Communications and Media Authority having day-to-day management responsibilities such as implementing spectrum allocations. These respective roles were clarified in 2021 reforms to the *Radiocommunications Act 1992* (Cth) (DITRDC 2022c). The current spectrum allocation system for mobile broadband purposes does not appear to be a barrier to productivity-improving uses of technology and data. As the use of mobile internet continues to increase, particularly as 5G enables more widespread economic applications, it will be important that the allocation system continues to support the highest value uses of spectrum assets. This could require an examination of how spectrum is allocated to other uses, such as for television broadcasting or government purposes (for example, defence).

fixed networks [although] recent trends highlight that mobile data downloads are growing faster than fixed downloads' (BoCAR 2020, p. 74). In this context, the ACCC has recently stated that:

> 5G mobile and fixed wireless services could become a substitute for fixed line broadband services [and] in some areas are becoming increasingly attractive to consumers as an alternative to fixed line services. However, the technology currently has a limited geographic footprint and it is not clear whether it could service the majority of fixed line broadband end-users. (ACCC 2021d, p. 12)

As such, investing in a mix of technology types to improve regional and remote connectivity is most efficient, as different connection methods can be used and adapted to more efficiently accommodate the needs of various locations. The Commission has previously advocated for a technology-neutral approach to government policy on connectivity in its 2017 *Telecommunications Universal Service Obligation* inquiry, noting that arrangements should be technologically neutral to allow for cost-effective solutions (PC 2017b, p. 12), and could include a mix of fixed broadband networks, mobile coverage and satellite services.

The Australian Government currently invests significant amounts in regional digital infrastructure across a range of connection types. Larger national infrastructure programs generally have a strong emphasis on improving regional and remote connectivity, and funding is also allocated to specific regional initiatives.

- The National Broadband Network (NBN) provides broadband infrastructure and access to all Australian premises, predominantly using fixed line connections (representing 92% of its network). A small share of premises are serviced via fixed wireless (5%) and satellite technologies (3%) (DITRDC 2021b, p. 1) — many of these are located in regional and remote areas, 'where premises are spread out geographically over many square kilometres' (NBN 2022). The initial rollout represented a $51 billion infrastructure investment (NBN 2020).
- The Mobile Black Spot Program (MBSP) seeks to improve mobile coverage across Australia. The government co-invests with industry to encourage mobile network operators to build mobile infrastructure in areas with limited connectivity. Most MBSP sites are in regional and remote areas (figure 3.3), and for some mobile network operators, the majority of regional and remote sites they built in 2021 received government co-funding (ACCC 2021b, p. 12). In total, the government's $380 million funding commitment to the MBSP has 'generated a total investment of more than $875 million, to deliver more than 1,270 new mobile base stations across Australia' (DITRDC 2021a).
- The Regional Connectivity Program (RCP) provides grants for 'place-based' telecommunications infrastructure projects in regional and remote Australia. Grants have been provided for a mix of technology types, including projects to deploy new mobile sites and to upgrade or extend fixed networks, some of which also involve industry co-investment. More than $250 million of government funding has been committed to the RCP's two rounds (DITRDC 2022b).

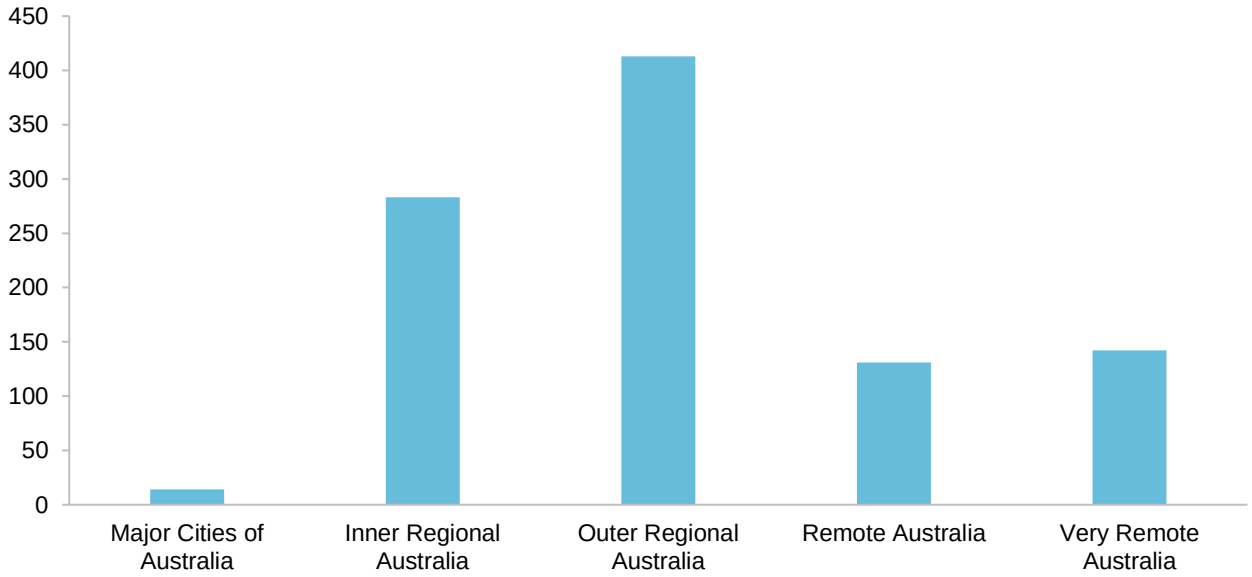
At the same time as this significant government investment, there is also substantial private sector activity in developing regional digital infrastructure in Australia.

- Telstra announced a total investment of $350 million in 2021 to improve its regional and rural networks, predominantly to enhance and extend mobile coverage. This funding was said to be in addition to the projects that Telstra had co-invested in with the Australian Government at the time (Penn 2021).
- Telstra has also partnered with satellite communications companies ViaSat and OneWeb to offer its own satellite services, in competition with the NBN (Burns 2022; Griffith 2022).
- Starlink's satellite internet services are available in some parts of Australia. The company has ground stations — which connect to its satellites to provide internet services — in New South Wales, Victoria, Queensland, South Australia and Western Australia, and a licence from the Australian Communications and Media Authority (ACMA) to sell its services Australia wide (ACMA 2021b; Fogg 2022).

- HyperOne announced a $1.5 billion investment in 2021 to build a 20 000 km network of optic fibre cable connecting every Australian capital city. The network would have 'more than 1000 "on-ramps" in regional and remote Australia' (Crozier 2021), which would improve connectivity in these areas.

Figure 3.3 – Most Mobile Black Spot Program sites are located in regional and remote Australia

Number of MBSP sites by location, 2022



Source: ACCC (2022h, p. 14).

Government investment in regional digital infrastructure should therefore be targeted towards addressing infrastructure gaps, where required, without unduly interfering with private sector activity. As the Commission stated in its 2017 *Telecommunications Universal Service Obligation* inquiry:

> … 'market gaps' or 'market failures' do not in themselves provide a case for government intervention, because such interventions typically generate costs as well as benefits to the community — both directly and indirectly. A case can be made for government to intervene only where there is a net benefit to the Australian community. The relative merits of policy options should then be assessed against cost-effectiveness criteria including:
>
> - the cost to the community of achieving a minimum quality of service
> - technological neutrality
> - impacts on competition and incentive effects on service providers
> - administrative costs and regulatory compliance burdens, with regard to flexibility to adjust to future developments. (PC 2017b, p. 6)

Finding 4.9
Technological change has led to increasing options for internet connectivity

The suitability of fixed and mobile broadband, and satellite technology, as options to reliably connect to the internet differs substantially across Australia. The market for internet connectivity is evolving rapidly, with a range of private sector providers developing regional digital infrastructure that may address some access and reliability gaps.

Better data would assist in linking investment to outcomes

Understanding the genuine gaps where government investment would result in a net benefit to Australian businesses and individuals requires good data about not just the demand for connectivity in regional and remote areas, but also the quality and adequacy of connection options. Indicators such as internet access, upload and download speeds, packet loss and latency need to be analysed at a regional and local level in order to properly identify gaps and target government investment (IA 2022a, pp. 80–99).

Much of the data publicly available on internet coverage and speeds is in aggregate across Australia — for example, the Ookla Speedtest or M-Lab data (section 1.2), though this data suffers from selection issues (AlphaBeta 2019b, p. 9), and data about fixed and mobile broadband use in the ACCC's *Internet Activity Report* (ACCC 2021a), which overcomes selection issues. There is also some aggregate data on internet quality, with the ACCC's *Measuring Broadband Australia* report publishing data on latency, webpage loading time and packet loss frequency for fixed line connections across Australia (ACCC 2022g, pp. 20–22). While these aggregate datasets can be useful, they do not provide sufficiently granular information for targeting location-based investments towards regions where there are gaps in access and service quality.

The information that is currently published on geographic disparities in internet quality and adequacy is limited. There is locational data available on NBN coverage by type of connection (such as fixed wireless broadband connections, DITRDC 2020), but this provides little information about the geographic variation in the quality of connections that are actually used by individuals and businesses. The ACCC has reported that regional outcomes are generally poorer than urban outcomes for fixed broadband services. For instance, the average download performance in regional areas was 95% of advertised plan speeds compared with 98% for urban areas, and the average latency in regional areas was 13.0 milliseconds compared with 10.7 milliseconds for urban areas (ACCC 2022g, pp. 27, 30). However, beyond the broad geographic classifications of 'urban' and 'regional', there were no further breakdowns that would enable poor outcomes to be identified at specific locations across regional Australia.[10]

On mobile broadband connectivity data, the ACCC requires mobile network operators to 'report on the locations of their core network and customer access network' under the Audit of Telecommunications Infrastructure Assets — Record Keeping Rules (ACCC 2022e). The maps that are published by these operators provide some information about the availability of mobile coverage in specific locations and the potential quality of connections (based on predicted 3G, 4G or 5G coverage; actual speeds are not part of these maps). The ACCC has observed that their efforts to improve disclosure of data on mobile connectivity outcomes provide 'useful information on the state of mobile networks for policymakers, particularly when formulating policy responses to mobile coverage issues' (ACCC 2021b, p. 2). Telstra submitted that mobile network coverage data tends to depict availability rather than speeds because 'with fixed networks there is capacity to readily observe and report on service standards consistent with plans sold in the market, but mobile networks are not amenable to this given the issues of variability and contention… noting mobile plans are typically sold based on data allowances as opposed to speeds' (Telstra, sub. 174, p. 23).

Ultimately, geographic breakdowns of internet connectivity, quality and adequacy are not available at a sufficiently granular level to measure digital infrastructure gaps and inform targeted government

[10] This is broadly comparable to the geographic granularity available in other developed countries' internet speed data. For example, the Measuring Broadband America reports publish national statistics about measured download speeds, latency and packet loss for selected internet service providers (FCC 2021). The Measuring Broadband Canada program adopts a similar approach to collecting performance data as Australia and the United States (CRTC 2020). In the European Union, the *Digital Economy and Society Index* includes country-level data on the share of households with broadband connections above particular thresholds (2 Mbps, 30 Mbps, 100 Mbps, 1 Gbps) (EC 2021a).

investment.[11] To inform its assessment of broadband and mobile connectivity gaps in the Regional Infrastructure Gap Prioritisation Framework (discussed above), Infrastructure Australia undertook extensive surveys, submissions and regional workshops (IA 2022b, p. 21). A more comprehensive and granular source of data about connectivity outcomes, collected on an ongoing basis, would improve location-based decisions for the public and private sectors about how and where to invest in regional digital infrastructure.

In addition to informing investment decisions, improved data on internet speeds would also enable more informed regulation. The Australian Government has implemented a Universal Service Guarantee (USG) requiring that 'all Australians [have] access to broadband as well as voice services' (DITRDC 2021b, p. 1).[12] The guarantee includes minimum standards for peak broadband speeds, and these needs are likely to change over time as demand for data and connectivity increases in the future. As such, the *2021 Regional Telecommunications Review* recommended that: 'the minimum USG standards, including download/upload speeds and performance during peak or busy hours, will need to increase and should be subject to an annual review, particularly for consumers outside the NBN fixed line footprint' (RTIR Committee 2021, p. 12). This would be most effectively paired with better data on connection access, quality and adequacy.

But collecting this data at a granular geographic level is not a straightforward task. For instance, in its analysis on mobile connectivity in its *Mobile Infrastructure Report 2021*, the ACCC noted that assessing mobile coverage by location can be challenging because 'the mobile network operators use predicted coverage as the basis for their coverage maps, and their input assumptions and metrics are different. They can also change input assumptions from time to time, which makes it difficult to accurately assess coverage changes' (ACCC 2021c).

Data about the ability for individuals and businesses to use the internet would ideally be collected based on the desired outcome — that is, whether access to and the quality of connections is fit for purpose. Consistent outcomes data about internet access and the quality and adequacy of connections in particular areas, across all types of connections (fixed broadband, mobile broadband and satellite), would facilitate technology-neutral decisions about what investments are most appropriate for specific locations where government funding may be required.

Improving transparency on how investment decisions are made

Despite the significant government investments in regional digital infrastructure (discussed above), there is a lack of transparency about how these investments are made and which priorities are pursued. Allocating funding under programs such as the NBN, MBSP and RCP to specific areas or connection types means less funding available for investment in another location or technology. There is limited transparency about how such trade-offs have been weighed and if decisions made appropriately considered the relevant benefits and costs.

[11] The analysis in this chapter is primarily based on publicly available data about connectivity outcomes. It is unclear whether providers and/or regulators have access to unpublished information at a more granular geographic level.

[12] The USG's reference to voice services reflects the fact that it incorporates the old Universal Service Obligation (USO), which guaranteed access to landline telephones and payphones. The inclusion of broadband services in the USG, which was first announced in 2017 as part of plans to replace the USO, was intended to align the guarantee with the 'significant changes in technology, the marketplace and customer preferences' (DCA 2018, p. 7) that have taken place in more recent years — with reliable access to internet now essential for participating in the modern Australian economy and society. The technology options that are now available to deliver internet (discussed above) are also able to provide voice services, either directly or effectively as a by-product of data services (e.g. voice calls via the internet).

For example, although the Department of Infrastructure, Transport, Regional Development, Communications and the Arts assesses RCP grant applications based on publicly available program guidelines (DITRDCA, sub. 201, p. 10), the Australian Communications Consumer Action Network:

> … expressed concern regarding the Federal Government's Grant Guidelines for the RCP Round 2 … [it] considers whether the project supports a government priority without clearly defining what the government priority may be, in addition to the Department reserving the right to recommend funding a project which may be lower ranked against merit criteria. Stipulations such as this within grant guidelines adds uncertainty and reduces transparency from the grant process. (ACCAN, sub. 118, p. 7)

And while it is clear that much of the MBSP program targets investment in regional and remote areas (figure 3.3, DITRDC 2021a), and the government publishes data about community-reported mobile black spots (Australian Government 2021b), there is opacity about how the mobile sites are prioritised and selected for government investment. The Commission previously recommended in 2017 that transparency in funding decisions could be improved by:

> … commission[ing] an independent evaluation of the Mobile Black Spot Program. Such an evaluation should consider measures to improve the program's operation, to best ensure that the program's objectives are prioritised and site selection is evidence-based. (PC 2017b, p. 23)

This recommendation was not accepted by government.

A similar case can be made for improving transparency about government decisions on providing funding to the NBN. For instance, the 2022-23 Budget included a $480 million grant to upgrade the NBN's fixed wireless towers, which will improve broadband speeds and increase data allowances for some users (DITRDC 2022a). In addition, the government announced in October 2022 that it will provide a $2.4 billion equity injection to expand fibre-to-the-premise connections to a further 1.5 million premises. In both cases, funding has been allocated without a competitive process, with the claim that 'given the investment to date in the network and the incremental cost of upgrading it and the other options available, the Government considers this is a value for money investment' (DITRDCA, sub. 201, p. 7). However, it is unclear how the decision was made to allocate government investment towards these connection types or locations. It will be important that these upgrades are accompanied by transparency about how and why they are to be undertaken, to ensure taxpayer funds are being spent efficiently.[13]

In addition, State and Territory Governments also make significant investments in regional digital infrastructure that would benefit from increased transparency about how funding decisions have been made. These include the Connecting Victoria Program, NSW Regional Digital Connectivity Program, WA Digital Connectivity Program and South Australia's Mobile Network Extension Devices Pilot Program (Gary McLaren, sub. 137, p. 5).

Periodic independent reviews of digital infrastructure programs such as the RCP, MBSP and NBN would increase the likelihood that government funding for such investments is allocated to those specific locations and technology types that would yield the highest benefits for the community. Evaluating these investments

[13] In addition to individual grants and equity injections, the NBN also receives funding for its loss-making fixed-wireless and satellite services through an internal cross-subsidy that is supported by the Regional Broadband Scheme levy. In the Australian Government Competitive Neutrality Complaints Office's investigation of NBN Co, the Commission recently observed that the government could replace this levy arrangement with direct Budget funding for these non-commercial services (an option that has also previously been suggested by the ACCC) (PC 2022, p. 41). This would provide more transparency about the costs of providing these services. It may also be used to transition towards the more competitive funding arrangement discussed below, whereby the direct funding could eventually be made available to the provider that can deliver the required services in the most cost-efficient way, as identified through a tender mechanism.

would also enable governments to assess whether current funding allocations and policy settings are appropriate as demand and supply in the market changes for other reasons — for example, strong population growth in particular towns or increased private sector investment in regional digital infrastructure. This allows governments to adjust their investments accordingly over time.

Technology improvements could enable more competitive funding arrangements

Given the complex technology- and location-specific aspects of connecting regional and remote Australia to the internet, there may be a more efficient way for government to fund digital infrastructure investments. It can be difficult for the government to decide on the type of infrastructure that would most cost effectively deliver the USG's minimum standard in a given location. The government could instead consider using a technology neutral market-based mechanism such as competitive tendering, which may lead to more efficient outcomes and address gaps in regional and remote connectivity at lower cost. The mechanism could also be designed to promote data collection on service outcomes and transparency on funding decisions.

For example, instead of allocating regional digital infrastructure funding through programs such as the NBN, MBSP and RCP, the government could offer to pay the lowest-bidding service provider to deliver connectivity to a particular area, defined at the regional level, subject to conditions such as minimum service standards and maximum prices charged to consumers. The government would have flexibility in defining these conditions across different regions; for example, there may be equity or social inclusion reasons (discussed above) for requiring relatively lower price caps in very remote areas, if people have less ability to pay for basic internet services in these locations. Tenders could also be designed to give service providers flexibility to realise economies of scope across different regions, such as by allowing combinatorial or package bidding, so that providers can bid for a package of locations where there might be efficiency gains from supplying all of these areas together.

Successful tenders may include an upfront payment, with full funding to be provided over time as the provider delivers on their commitment — contracts should therefore be of a sufficient length for service providers to earn a return. A new tender would be issued after this period to ensure providers remain competitive. If thin markets are an issue and the call for providers in a particular location leads to only one party being willing to participate in the tender, the government may need to enter into individual negotiations with that provider — effectively the provider of last resort — to avoid being held captive by that one party.

The intent of such a mechanism would be that government pays the least-cost private provider to guarantee a minimum service level in each location, with the cost to government determined by the market. It would not preclude other private sector providers from competing in that region, such as by offering more advanced or niche products that consumers may be willing to pay more for, or if they lower their costs by investing in new technologies over time.[14]

The Commission has previously recommended competitive tendering for public infrastructure and services provision, noting that it creates incentives for providers to keep prices closer to the cost of delivery (PC 2014,

[14] This section's discussion about competitive tendering for the USG is focused on connectivity in regional and remote Australia, as it is in these areas that the government's activity would have larger benefits in delivering more efficient outcomes. The 'universal' aspect of the USG means that the Australia-wide mechanism would apply to metropolitan areas as well, with a tender offered for each metropolitan location (just as regional and remote tenders would be defined by location). However, as the higher population density in metropolitan areas means that it is generally commercially viable for multiple broadband service providers to co-exist and compete (for example, ACCC 2021d), in practice a competitive tender for these locations would be bid down to zero.

2015, 2017b). In its *Telecommunications Universal Services Obligation* (USO) inquiry, the Commission also observed that a tender mechanism for these specific services should:

- specify service requirements as outcomes rather than prescriptive inputs, technologies or processes, as this encourages innovation and lower-cost service delivery
- require clear performance reporting to allow for provider accountability and enable government to identify gaps in service provision
- acknowledge the advantage that incumbents or dominant providers have in tendering, and avoid discriminatory service requirements (PC 2017b, p. 260).

In considering the design of a tender mechanism for funding digital infrastructure investment to deliver the USG (which replaced the USO), similar principles apply. For example, outcomes-based requirements for reliable and good quality internet services could include upload and download speeds,[15] latency or even the ability to access essential services online (such as telehealth). And existing data about service outcomes could be improved as part of implementation, such as by requiring service providers to self report outcomes as part of the tender's performance reporting requirements, complemented by independent assessments of internet reliability and quality.

In relation to existing providers that may dominate the regional digital infrastructure market, some service providers already observe that Telstra and NBN Co are large incumbents in regional and remote Australia.

- Competitors have argued that Telstra's physical line network, partly funded through government subsidies over the years, provides advantages in delivering mobile services as it supports greater backhaul capacity in regional and remote areas (Optus 2016, p. 23). As such, even though the MBSP uses tenders to allocate funding, 'in reality Telstra faces little competition across areas where other mobile network operators lack backhaul capacity to support the cost-effective rollout of these new base stations' (VHA 2016, p. 12).
- Previous government funding and policies aimed at subsidising the NBN in regional and remote areas could provide NBN Co with a competitive advantage. For example, the Regional Broadband Scheme was created to 'fund the financial losses of NBN Co's fixed wireless and satellite networks' (ACCC 2020, p. 1), requiring telecommunications providers to pay a levy to NBN Co for each premise they supply with a designated broadband service over a local access line owned by the provider (ACMA 2021a). This disincentivises providers from building and using their own fixed line infrastructure (Boyd 2021).

The government trialled a market-based mechanism to deliver the USO in 2001 to reduce costs, increase transparency, improve performance and compliance, and encourage new providers to enter regional markets (Jackson 2000). However, the trial was not a success as no providers participated in the scheme:

> Under this pilot program, carriers could nominate to be a universal service provider in one or both of the two nominated areas and would receive a set subsidy for each customer they supplied in that area. Carriers were required to supply any individual requesting a service within the nominated area, which meant that potential competitors were required to have a network capable of supplying every individual within the area. No carrier nominated to become a universal service provider under this scheme. (ACCC 2007, p. 12)

The ACCC later observed that competitive tendering for the USO had become more feasible in the years following the 2001 trial due to technological advances (ACCC 2007, p. 12, 2016, p. 7). With further

[15] As an international example, in July 2022 the Chairwoman of the US Federal Communications Commission suggested that the national standard for minimum broadband speeds be increased from 25 Mbps to 100 Mbps for downloads, and 3 Mbps to 20 Mbps for uploads. Chairwoman Jessica Rosenworcel also proposed that the FCC 'consider affordability, adoption, availability, and equitable access as part of its determination as to whether broadband is being deployed in a reasonable and timely fashion' (FCC 2022).

advancements in technology and increasing competition in the broadband market (across fixed, mobile and satellite connections), the government may be in a better position to deliver the USG through tender.

Participants to this inquiry expressed mixed views on whether such a tender mechanism would work in practice at the present time. Several stakeholders observed that delivering the USG via competitive tender would encourage internet connectivity to be delivered at lower cost from a range of providers; foster competition by providing opportunity to smaller industry players; improve the transparency, accountability and efficiency of government investment; and enable more extensive data analysis to inform investment decisions (ACCAN, sub. 118, p. 8; Gary McLaren, sub. 137, p. 8; IAA, sub. 168, p. 2). And some stakeholders also highlighted low earth orbit satellites as a particular type of technology that is already being offered in Australia and could change the way that the USG is delivered in regional and remote areas (Gary McLaren, sub. 137, p. 6; NBN Co, sub. 147, p. 12; Vocus Group Ltd, sub. 121, p. 2).

However, questions remain regarding whether technology and market competitiveness have sufficiently developed in regional and remote areas to feasibly implement a competitive mechanism for the USG at the current time. Although this section has outlined various examples of private sector investment in regional digital infrastructure and new providers entering the overall Australian market, it is unclear whether they would elect to participate in tenders to deliver the USG across all or most of the regions defined by the government. The Department of Infrastructure, Transport, Regional Development, Communications and the Arts observed that for smaller service providers and start-ups, 'their capability and long-term sustainability would need to be considered closely. The implications of providers cherry-picking more lucrative or desirable markets would need to be considered' (DITRDCA, sub. 201, p. 14). And NBN Co noted that:

> … there may be a tension between allowing private participants to selectively pick (by tendering) specific areas to serve and the efficiency with which less commercial areas can be served. Economies of scale are critical to development and deployment of telecommunications infrastructure … At present, neither vertically integrated smaller providers nor bigger foreign players are likely to have on-ground service and support capabilities to adequately serve large or multiple parts of regional Australia. (NBN Co, sub. 147, p. 8)

Transitioning existing government funding arrangements for regional digital infrastructure to a tender mechanism would lead to more efficient outcomes, but moving too early before technologies and markets are sufficiently developed to support a more competitive approach to funding risks failure. The government should therefore seek to transition towards such an arrangement once it is feasible, and could undertake market testing to understand whether this is possible now or, if not, at what point in the future implementation would be appropriate given the expected trajectory of technological and market development. Such an assessment could be undertaken by the ACMA and/or the ACCC.

Finding 4.10
Government investment in regional digital infrastructure often lacks transparency

Current funding arrangements for regional digital infrastructure involve government decisions about the types of technology and locations receiving public investment, and these decisions often lack transparency. Productivity-enhancing access to low-cost and reliable internet services could be delivered through a more competitive and transparent approach that facilitates market participation by a range of providers, such as through competitive tendering. Tenders could be technology neutral and adapted to different regional and remote community needs (on service outcomes and price), but the approach requires sufficient technological and market development to be feasible.

Recommendation 4.1
Better access to digital infrastructure in regional communities by improving funding mechanisms

The Australian Government should more efficiently and transparently fund digital infrastructure investments to motivate improved provision in Australia's regional communities.

This would ultimately require a transition in funding arrangements from the current patchwork of programs to a single market-based tender mechanism for delivering the Universal Service Guarantee, once the market for internet connectivity services across all technology types (fixed line, mobile, satellite) is sufficiently competitive to support such an arrangement.

The government should request that the Australian Communications and Media Authority and/or the Australian Competition and Consumer Commission undertake market testing to understand whether it is currently feasible or, if not, when technology improvements and new market entrants would enable a more efficient tender mechanism to be implemented.

In the meantime, governments should improve transparency about how funding is allocated for existing regional digital infrastructure programs, including publishing the reasons for funding decisions and evaluating the outcomes of previous investments.

3.2 Creating new data sharing and integration opportunities

There have been several government initiatives to improve data sharing since the Commission's 2017 *Data Availability and Use* inquiry (PC 2017a): box 3.1 describes actions for sharing government data, while the Consumer Data Right (CDR) is discussed in the section below. The strong focus on sharing public sector datasets is consistent with global policy activity — an OECD survey of 205 data sharing initiatives across 37 countries found that 'the large majority of government initiatives focus on access to and sharing of public-sector data (almost 65% of all initiatives), with the majority of these initiatives aiming at enabling open access to government data' (OECD 2019, p. 117).

Box 3.1 – Recent initiatives to improve public sector data sharing

The Australian Government has implemented a national regime for sharing public sector data through the *Data Availability and Transparency Act 2022* (Cth) (DAT Act). The Act facilitates data sharing from 'data custodians', which are generally Commonwealth agencies, to 'accredited users', who have been approved to receive data for the purpose of improving service delivery, informing policy development and/or research. The legislation also establishes the National Data Commissioner, an independent regulator responsible for overseeing the data-sharing scheme and broader education activities about public sector data sharing and use (ONDC 2022).

The proposed data sharing model in the original DAT Bill allowed for public sector data to be shared with the private sector. However, following amendments, the legislation that was passed specified that

Box 3.1 – Recent initiatives to improve public sector data sharing

industry and other private organisations are not allowed to participate and receive data in the scheme (Sadler 2022). As the reason for initially excluding the private sector was to establish the scheme and allow it to mature, some stakeholders have observed 'it may be that following further review, the DAT Act will eventually be expanded to allow private sector organisations to receive public sector data' (Catania, Wheelahan and Mani 2022). The Act stipulates that there will be a review of the scheme in three years, along with a five-year sunset clause.

The DAT scheme underpins the government's *Australian Data Strategy*, which was released in May 2021 (PMC 2021b). The strategy and its supporting action plan (PMC 2021a) outline the Australian Government's three data priorities — enabling greater data use, improving data safety and security, and maximising the value of data — and highlight how separate government initiatives and policies align with these priorities. Government investments in specific datasets and infrastructure mentioned in the action plan include:

- the Data Integration Partnership for Australia program and creating the Multi-Agency Data Integration Project (MADIP) and Business Longitudinal Analysis Data Environment (BLADE), which respectively link the government's people-based and business-based datasets for policy research. These have been used to inform the COVID-19 vaccine strategy by sociodemographic cohorts, measure the employment and social outcomes of vocational education students, and examine the benefits of government support for Indigenous environmental programs (ABS 2022a, 2022c)
- the Digital Atlas of Australia, an interactive online platform that will link Australian Government datasets based on location, to be beta-tested in mid-2023
- sector-specific initiatives in areas such as collecting and sharing freight data, modernising waste data visualisation, integrating regional datasets and gathering more geoscientific data on Australia's resources.

Separately, the *Intergovernmental Agreement on Data Sharing* was signed by the Australian and State and Territory Governments in July 2021. All jurisdictions have committed to sharing public sector data 'as a default position, where it can be done securely, safely, lawfully and ethically' (National Cabinet 2021, p. 1). Data will be shared under existing privacy laws (including the *Privacy Act 1988* (Cth) and state and territory privacy legislation) for the purposes of 'informing policy decisions; designing, delivering, and evaluating programs; tracking implementation; and/or improving service delivery outcomes' (National Cabinet 2021, p. 2).

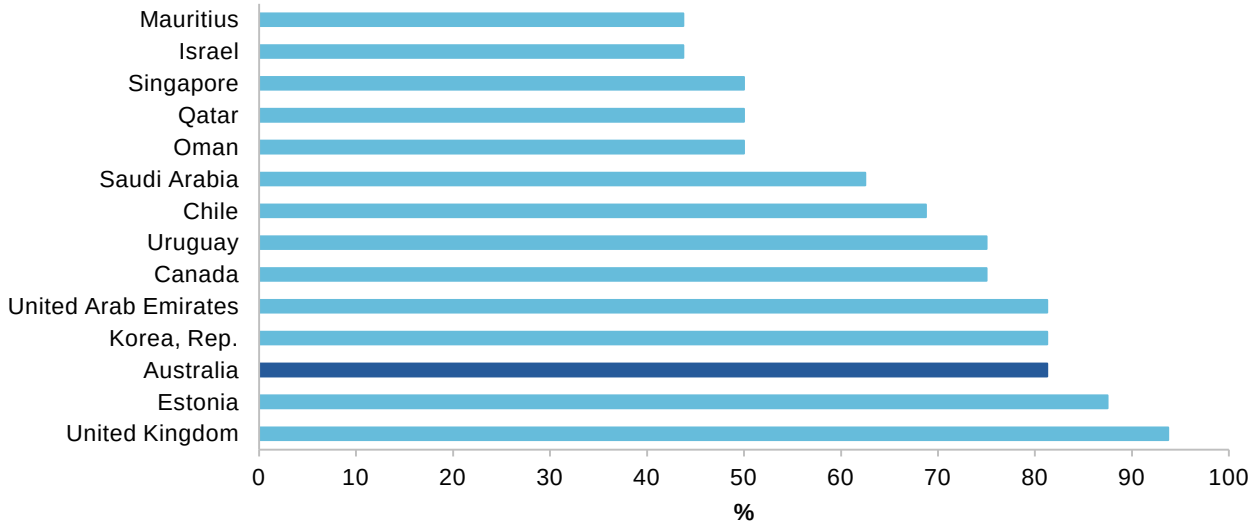
Australia performs relatively well on government-facilitated data sharing compared with other countries. For example:

- the UN's *E-Government Survey 2020* reported that Australia has a 'very high' level of open government data, based on an index examining countries' foundational policy frameworks, data-sharing platforms and data availability in various sectors (UN DESA 2020, pp. 258, 317)
- the Global Open Data Index 2016/2017 ranked Australia as second out of 94 countries on the publication of government data, with particularly high scores in the availability of national statistics, high-level budgets and geographical information (such as maps and administrative boundaries) (Open Knowledge Foundation 2017). However, Australia performed poorly on publishing detailed transactional data on government expenditure
- the World Bank's 2021 Global Data Regulation Survey examined 80 countries on 37 data-related policies, including 16 enablers of data sharing that relate to accessing public intent data and reusing private intent data (World Bank 2021b, ch. 6). High-income countries had adopted more enablers than middle- and low-income countries, and Australia ranked highly relative to other high-income countries (figure 3.4).

However, while Australia has some data sharing frameworks and infrastructure in place, there is still significant room for improvement to generate value and productivity growth from the use of data accessible under these frameworks. This includes increasing the number of organisations and individuals able to take up new opportunities to access and use data under these frameworks, and improving data availability and sharing in sectors of the economy where data remains relatively inaccessible but there is potential for significant benefit. It is particularly important to act now to leverage the increasing volumes of data that are being generated as more economic activity is digitised, including since the COVID-19 pandemic (as discussed in chapter 1).

Figure 3.4 – Australia has relatively mature data enabler policies

Share of enabler regulatory practices adopted by high-income countries, 2021[a]



a. Estimates are based on the Global Data Regulation Diagnostic Survey Dataset 2021, published by the World Bank. The dataset includes five data enabler policies relating to e-commerce, seven relating to public intent data and four relating to private intent data. Where the dataset includes multiple responses for a single policy, these responses have been aggregated to a single measure for that enabler. For example, a country is deemed to have common technical standards in place for government entities if it mandates at least one of the four types of standardisation options; it is not necessary for the country to have all four in place.

Source: World Bank (2021a).

More value from consumer data portability

The amount of data produced and analysed by the private sector has continued to increase rapidly since the Commission's 2017 *Data Availability and Use* inquiry (PC 2017a, p. 80). The potential to use this data to improve decision making, tailor services for customers and generate operational efficiencies is now well established. Governments can support greater sharing and use of consumer data through data portability policies, enabling consumers to authorise businesses holding their data to provide that data to third parties. Australia's Consumer Data Right (CDR) is an important example of enabling data portability for consumer benefit (box 3.2). To avoid disincentivising data collection and use (section 2.2), portability should be limited to data that is jointly produced by consumers and businesses through transactions between these parties, rather than being required for data that businesses have analysed and added value to. Australia's approach to consumer data portability is 'unique [compared with other countries] in its commitment to implement

economy-wide standardisation of consumer data with the only limits to the range of services enabled by CDR being "the imagination of entrepreneurs"' (Buckley, Jevglevskaja and Farrell 2022, p. 26).

Box 3.2 – The Consumer Data Right rollout is progressing

A Consumer Data Right (CDR) was enacted by the Australian Government through the *Treasury Laws Amendment (Consumer Data Right) Act 2019* (Cth). The CDR is being rolled out in stages, with ongoing consultation with industry and other stakeholders being a key part of the staged rollout.

The banking sector was first to be designated for the CDR in September 2019. Data sharing requirements were gradually phased in, starting with product and customer data on individual accounts, followed by information about business finance. The rollout was also staged such that the major banks were required to commence their data sharing obligations before non-major banks (Australian Government 2021a). As at mid-December 2022, there were 38 accredited data recipients (ACCC 2022b) and 114 active data holders (Australian Government 2022).

Implementation for the energy sector, which was designated in June 2020, is in progress. The rollout is another staged approach whereby product and customer data sharing obligations first commence for the three largest energy retailers, Australian Energy Regulator and Australian Energy Market Operator. Sequencing of the energy sector rollout, which began in October 2022, 'aims to ensure that CDR obligations first commence with participants that will provide the greatest coverage to enable consumers to benefit' (Treasury 2021a, p. 4).

Telecommunications was the most recently designated sector in January 2022. Similar to banking and energy, the information that will be shared under the CDR includes product and customer data, with the government planning to consult with industry on the rules and standards to apply (Kwan 2022).

Several recent reviews have examined opportunities to expand the CDR framework.

- The 2020 *Inquiry into Future Directions for the Consumer Data Right* examined how to expand the CDR's functionality and link CDR infrastructure with the broader data and digital economy (Farrell 2020). Its 100 recommendations included reforms to implement action initiation, such as payment initiation and account switching (discussed below). The government has agreed or agreed-in-principle to 94 of the inquiry's recommendations (Treasury 2021b).
- In late 2021, the Commonwealth Treasury undertook a Strategic Assessment on the next sectors and datasets that should be covered in the CDR rollout. It concluded that open finance should be the next area of focus, targeting high-value datasets from the superannuation, general insurance, merchant acquirer and non-bank lending sectors, as well as complementary data held by governments (Treasury 2022b).
- The Statutory Review of the Consumer Data Right, released in September 2022, reiterated the potentially significant impacts of action initiation under the CDR. For example, the CDR could facilitate digital payments as 'its unique framework for secure transfers of consumer, product and service data can integrate with and augment existing and emerging payment channels' (Treasury 2022c, p. 5).

While the CDR rollout is progressing and providing strong foundations for consumer data sharing, a great deal of the value that could be created from this data portability has yet to be realised. For example, in the banking sector, there are only 38 accredited data recipients and development of innovative products or improvements to customer service based on the CDR appear to be in their early stages still.

Some reports suggest that service providers are starting to replace 'screen-scraping' methods of collecting customer data (which are unregulated, more costly and less secure) with accessing higher quality information through the CDR. One fintech has observed that the CDR's 'cleaner set of data … is important as we look to add insights to help the emerging customer experience — like instant decisioning, straight-through-processing, or various nudges lenders can make to consumers' (Eyers 2022b). However, variable data quality from some banks and the time required to fix these issues (sometimes more than a week) may slow uptake (Eyers 2022a). The ACCC introduced a CDR sandbox in July 2022, providing an environment for potential and current CDR participants to test their CDR offerings and solutions, which could assist in improving data quality (ACCC 2022a).

Expanding the CDR's sectoral coverage and incorporating additional functions will create new uses of and therefore value from the data. Gemaker submitted that 'extend[ing] more rapidly the Consumer Data Right regime implemented for banking and energy – which has provided a strong basis for citizen trust – into other sectors [would] promote digital innovations that deliver similar productivity and user benefits' (Gemaker, sub. 13, p. 3). In addition, enabling action initiation in the CDR has the potential to result in significant consumer benefits, including:

> … overcoming [consumers'] friction when carrying out actions with their providers, as well as behavioural issues such as status quo biases… and reduc[ing] the complexity, time and costs to consumers seeking to carry out actions. Action initiation could support a range of actions that may be undertaken on the consumer's behalf. These may differ depending on each sector but could include enabling [an] accredited person to initiate payments, update personal information, change billing delivery preferences, open and close accounts and assist consumers to switch from one provider to another. (Farrell 2020, pp. 19–20)

The government sought comment on exposure draft legislation to enable action initiation in late 2022. This would allow the CDR to 'create a new channel for consumers to instruct a business to initiate actions on their behalf and with their consent. These actions could include making a payment, opening and closing an account, switching providers and updating personal details (such as address) across providers' (Treasury 2022a, p. 1). Ultimately, making it easier for consumers to switch between products and providers will spur competition between businesses to deliver better services to Australian consumers.

Finding 4.11
The Consumer Data Right is a good foundation but has low uptake

The Consumer Data Right (CDR) provides a strong foundation for consumer data sharing, but relatively low uptake means its economic benefits are yet to be fully realised. Initiatives such as the CDR sandbox, which may improve data quality, and introducing action initiation could increase uptake in the future.

More value from data provided to government agencies

Notwithstanding the advances in data sharing over the past five years, there remains significant potential to improve — for the benefit of the community — the sharing, integration and use of data that is held by government agencies. While progress on the underlying frameworks and legislation has been made over recent years (box 3.1), some stakeholders observe that the cultural barriers preventing greater data sharing — which were highlighted in the Commission's 2017 *Data Availability and Use* inquiry — still exist today.

> The [Commission's 2017 inquiry] found 'a very real culture of risk aversion and risk avoidance in the public sector when it comes to data release'. Anecdotally, this culture of risk aversion and avoidance has changed little since then. … the main impediment to data sharing is still a cultural one, supplemented by a lack of clear agency-specific guidelines and guardrails as to what can be shared, to whom and in what circumstances. (Christie and Wong 2021)

It is important to think broadly about what data can be shared and combined, and the potential users who might create value from this data. This could include agencies from different levels of government (including local government) and universities, as well as benefits arising from cross-sector uses of data; for instance, businesses or not-for-profit organisations deriving value from combining their own data with government data. Breaking down silos between these groups, such as via data sharing agreements[16] or other partnerships (in the case of data users outside of the public sector and academia), could create new opportunities for data use.

Agencies that successfully embark on collaborative data sharing initiatives should be highlighted as examples where risk aversion has been overcome to yield benefits for businesses and individuals, as their experiences can provide lessons for others seeking to improve data sharing and use. The Australian Taxation Office (ATO) and ABS are prominent examples of how government agencies can lead the way in creating shared value using data they collect and hold, and the National Disability Insurance Agency (NDIA) has also commenced digital and data partnerships with the private sector in recent years (box 3.3).

Based on the experiences of these government agencies, features of successful arrangements that have created value via data sharing include:

- *Working with digital service providers to integrate data requirements into software products* that are already used by businesses, to reduce reporting burdens and maintain data quality. In implementing the Single Touch Payroll (STP) system, which captures near-real time payroll information entered by businesses in their accounting software, close collaboration between the ATO and digital service providers 'was a huge factor in the program's success' (DSPANZ, sub. 18, p. 2). The ATO set up a Digital Partnership Office to facilitate this collaboration. The NDIA has a Digital Partnership Program with a similar purpose.
- *Supporting businesses with more limited capacity or digital capability*. The ATO adopted a staged approach to implementing STP to assist employers through the transition: large employers were required to report via STP before small employers, and there were concessions for some businesses that needed more time, such as micro employers and seasonal employers (ATO 2021c, 2021a, 2021b). Meanwhile, the NDIA allows smaller service providers to connect to their data and systems via 'aggregator' software companies, enabling the benefits of improved data use to flow broadly across the sector, including to providers that would not have the capability to connect directly to the NDIA's systems themselves.
- *Considering innovative and high-value uses of data* across public and private entities, beyond meeting administrative and operational needs. For example, the ATO makes de-identified individual and business tax data available to be linked to other datasets in MADIP and BLADE, for research purposes (box 3.1). STP data is used to support government policy decisions and service delivery, including as a critical input for the government's economic response to COVID-19 (Hambur et al. 2022). The ABS is also seeking to combine and report data collected from businesses' accounting software back to businesses so that they can compare their performance against others.
- *Using data sharing to build relationships in the broader ecosystem*. In the Commission's consultations, one business described the ATO's leadership as a 'symbiotic relationship' with industry — the agency has enabled more data collection and sharing through STP and other digital initiatives, which has, in turn,

[16] The *Data Availability and Transparency Act 2022* (Cth) provides for accredited data users and data custodians to enter into data sharing agreements for the use of data in particular projects that serve the public interest.

allowed technology providers to create new value in the wider business ecosystem. And the NDIA's focus on digitisation and data has led to the formation of a Digital Community of Interest, where organisations share learnings and feedback about the change process.

Box 3.3 – Examples of government and private sector digital and data partnerships

The Australian Taxation Office (ATO) provides a case study on how government agencies can lead the way in creating shared value using data. Significant volumes of data must be collected from individuals and businesses every year as part of tax administration. The ATO sees data usage — and digitisation more broadly — as an opportunity to improve taxpayers' engagement with the tax system, by facilitating 'well-designed client experiences' in a system where it is 'easy to comply, but hard not to' (Hirschhorn 2021).

To improve digital uptake and support new uses of data, the ATO works with digital service providers (which provide accounting, tax and other software to businesses) to integrate data requirements into their software products, minimising reporting burdens while maintaining information quality. The agency has a Digital Partnership Office to support these collaborations with the private sector, which has enabled, for example, the co-design of software standards and security mechanisms (ATO 2019).

Moreover, the ATO's leadership in technology and data use has encouraged many Australian businesses to digitise and adopt potentially time-saving software solutions. For example, prior to the introduction of the Single Touch Payroll (STP) system, which commenced in 2018 and captures near-real time payroll information entered by businesses in their accounting software, about 48% of employers lodged their payment summary annual report with the ATO in a non-electronic format. Now in 2022, approximately 90% of employers interact electronically with the ATO in near real time as they run their payroll and report that information (ATO, pers. comm., 17 May 2022).

There are currently more than 300 STP product offerings listed on the ATO's online register of commercially available products (ATO 2022), and ecosystems of digital service providers have grown around the data that businesses are entering into their software platforms. For example, the cloud-based accounting software provider Xero underpins a platform of over 1000 apps. These apps take data that businesses enter into Xero, combine it with other sources and tools, and produce valuable insights such as cash flow forecasts, dashboard reporting, flagging risks and linking to e-commerce platforms. In 2020, each developer or app partner in this Xero ecosystem spent more than $20 000, on average, on innovations such as increasing efficiency, implementing new ideas and anticipating future needs (Xero 2021b, p. 15). The ATO has catalysed innovative activity in such ecosystems — it established and maintains the framework for collecting businesses' data, enabling software providers to push this data back to businesses in more valuable forms (with consent and appropriate protections).

The ABS is working with digital service providers to allow businesses to complete the Quarterly Business Indicators Survey through their accounting software from March 2023. Businesses will benefit in several ways: first, 'small and medium businesses will spend at least 70% less time completing ABS surveys'; and second, the ABS will be able to use and combine the collected data to 'provide tailored reports back to business to help them understand their performance against similar businesses' (ABS nd; PMC 2022a).

Government leadership in data sharing partnerships across agencies and sectors should not be limited to business transactions and accounting data. The National Disability Insurance Agency (NDIA) has a Digital Partnership Program, which 'manages controlled and secure access to some of the NDIA's data and systems … so providers and software developers can build new tools, applications and digital

Box 3.3 – Examples of government and private sector digital and data partnerships

marketplaces to improve how participants, providers and the NDIA all connect and work together' (NDIA 2020). The program had 240 digital partners as at June 2022, comprising directly connected registered providers (often larger service providers) and smaller providers that indirectly connect through 'aggregator' software companies (NDIA, pers. comm., 10 June 2022).

Provider access to the NDIA's application programming interfaces under the Digital Partnership Program has enabled the streamlining of a range of National Disability Insurance Scheme (NDIS) transactions. The provider adoption curve generally starts with lower-risk but prolific transactions, such as more visibility over NDIS participants' plans and service bookings, before progressing towards more complex transactions, such as claims processes, as providers build confidence in the streamlined processes. More broadly, a Digital Community of Interest — with over 20 organisations and members across providers, participants, peak bodies and software developers — enables learnings and positive changes to be shared among interested parties. The group meets multiple times a year, which provides opportunities for the NDIA to receive feedback on what is working and what to progress next (NDIA, pers. comm., 10 June 2022).

One area where there is opportunity to get more value from data provided to government, and increase digital uptake across the population, is the Australian Government's Digital Identity initiative. This is a voluntary, centralised system for identity verification when accessing online services. Individuals create a digital identity through accredited identity providers (including the ATO, Australia Post and Mastercard, with other providers to be added), which set up and manage a digital identity account, and credentials such as passwords are managed by accredited credential providers (DTA 2022b). The system is designed to preserve privacy using rules and standards set out in the Trusted Digital Identity Framework, with individuals sharing only relevant details and service providers unable to seek further personal information without consent.

The Digital Identity system aims to improve convenience, as individuals no longer need multiple logins to access different services, and security, as identity verification is centralised so separate service providers do not need to collect and store sensitive information such as driver's licence and passport numbers (Bennett and Davidson 2022; Shah 2022). Fewer reproductions of sensitive information reduces the risk of third-party losses of personal information to security breaches. This is especially pertinent in light of sensitive data breaches at some large Australian businesses in late 2022, such as Optus and Medibank. The head of Australia's Digital Transformation Agency noted that had there been 'a working identity system, Optus would not have had to hang on to all the personal data that is now in jeopardy' (Burton 2022a). These security benefits should be clearly communicated to Australians, to encourage adoption of the Digital Identity.

The Digital Identity system has seen some good uptake recently, with more than 8.7 million individuals on the system as at July 2022 (Hendry 2022), up from over 6 million as at December 2021 (Robert and Hume 2021). However, a key barrier to further uptake is the limited uses of the Digital Identity, which is currently only able to be used as a way for individuals to verify their identity for selected services provided by the Australian Government, such as applying for a tax file number or updating business details and authorisations on the Australian Business Register (Australian Government nd). Increasing the number of uses for the Digital Identity will also create 'network effects' whereby more organisations accepting a digital identity will encourage more users to sign up, which will in turn encourage more investment by organisations to accept the digital identity (Shah 2022, p. 8).

Uptake could be encouraged by allowing State and Territory Governments to use the Digital Identity for services where they require identity verification (such as for driver's licence applications), as well as the private sector (such as for bank or utility account openings). The Australian Government could work with the Council

on Federal Financial Relations to improve access to its Digital Identity for State and Territory Government services. Draft legislation required to expand the Digital Identity system was discussed and published in 2021 (DTA 2022a; Robert 2021), though it did not progress far from this point. As of November 2022, the Australian Government has signalled an intention to renew its focus on the Digital Identity (Shah 2022). This could potentially include integrating the system with the myGov mobile app to provide access to an expanded set of federal services in one environment, which could also provide a channel for further links with state government services and the private sector (such as banking, transport and corporate services) (Burton 2022b).

Avoiding duplication of identity verification systems is also important, as having multiple systems would hinder the consumer experience and limit the efficiency gains from a centralised system. The NSW Government is developing the NSW Government Identity Strategy, which has already rolled out digital driver's licences and will explore the NSW digital identity separate from the federal system (NSW Government 2021). It is important for the Australian Government to prioritise expansion of the digital identity system — and where possible learn from the experiences of New South Wales — so that it can be used for State and Territory Government services to avoid a proliferation of systems. The Australian Academy of Technology and Engineering has noted that different approaches across jurisdictions can lead to inefficiencies:

> When a new digital initiative commences it is important to undertake a systematic review of existing standards. However, this does not always occur … [for example,] digital driver's licenses in different jurisdictions. Application of existing standards will help minimise reinvention, … helping create nationally consistent approaches. (ATSE, sub. 89, p. 4)

Recommendation 4.2
Expanding use cases for the Australian Government Digital Identity

The Australian Government, working with the Council on Federal Financial Relations, should increase access to its Digital Identity so that State and Territory Government services that require identity verification (such as applying for a driver's licence) and private sector services that require identity verification (such as opening a bank or utility account) are able to use the system, with appropriate access controls and safeguards.

Governments should work towards adopting a single national digital identity, rather than different jurisdictions having fragmented identity systems that require citizens to verify their identity with governments and businesses through different channels.

Cross-sector data sharing policies

Broader data legislation and policy settings can also support collaboration and integration — or prevent it. One example is the CDR: as discussed above, its expansion into open finance will include not only private sector data but also customer-specific data held by government. The recent strategic assessment found that:

> Prioritising the inclusion of customer data held by governments recognises that most consumer milestone events or decisions (for example, buying a house, getting married, having a child, starting or winding up a business, or retiring) will involve a mixture of data held by private business and government agencies about an individual or business.
>
> … expansion to government datasets and the inclusion of government agencies as both data holders and accredited data recipients has the potential to improve private sector goods and

> services, support improved Government service delivery, and support Australians and Australian businesses across all facets of their lives and operations. (Treasury 2022b, p. 9)

On the other hand, the *Data Availability and Transparency Act 2022* (Cth) (DAT Act) does not currently allow for government data to be shared with the private sector, including businesses and not-for-profit organisations (box 3.1). This limits the ability for the data to be used for productivity- and welfare-enhancing purposes, such as for policy and research or to improve products and services.

For example, some not-for-profits that deliver local community services on behalf of the government have observed that more data sharing and government–private sector collaboration, such as via the Act, would enable them to improve program delivery and community outcomes (Sier 2022). The review into Australia's response to COVID-19 highlighted the importance of data sharing between the government and private sector in enabling the policy response, and recommended that private sector researchers should be allowed to access public sector data under the scheme subject to accreditation and other controls (Shergold et al. 2022, p. 65). And participants to this inquiry submitted that more access to government data by researchers, not-for-profits and data intermediaries, in a secure and trusted framework, can improve our understanding of and policy response to national challenges such as population ageing, disaster prevention and recovery, energy security and First Nations community issues (ATSE, sub. 89, p. 3; Seer Data and Analytics, sub. 139, pp. 3–4).

Sharing government data with businesses can enable improved products and processes, better business decisions and innovation (PC 2017a, pp. 106–108). For instance, retailer Best Buy has used government demographic data to develop a market segmentation strategy based on customised consumer profiles, while in the health sector, Propeller Health created a GPS-enabled tracker that monitors inhaler usage by asthmatics from data supplied by the US Centre for Disease Control and Prevention to improve patient outcomes (Chui, Farrell and Jackson 2014, p. 10). And the Commission has previously noted that superannuation member outcomes — for those in retirement or transitioning to retirement — could be improved by using higher quality public data to develop and price super fund products (PC 2018, p. 240).

The DAT Act does not currently allow private sector access because of the desire to balance increased data use against privacy and security concerns (ABS, sub. 127, p. 12). Therefore, any expansion of the DAT Act to allow private sector participation should be done gradually and with appropriate safeguards. This could, for example, include a staged implementation, whereby access is first made available to accredited private sector organisations using the data for policy and research purposes to achieve social objectives, before the scheme is eventually opened for businesses to use commercially. And in terms of the appropriate safeguards, the BSA Software Alliance observed that the DAT Act's existing accreditation framework for data access already allows the government to make risk-based decisions on whether an entity can meet the security and data-handling measures required to safely use the data, and that this framework could be applied to businesses and not-for-profit organisations as well. In addition, they noted that government can explore new privacy-enhancing technologies such as 'homomorphic encryption, differential privacy techniques, and federated machine learning [to] create opportunities for further sharing data while preserving individual privacy' (BSA, sub. 134, p. 3).

Another approach that has been applied in other countries to improve data sharing and use between governments, companies and researchers is data labs — 'agile implementation units with cross-functional expertise that focus on specific use cases. Solutions are rapidly developed, tested, iterated and, once successful, rolled out at scale' (Domeyer et al. 2021, p. 9). For instance:

- in the United Kingdom, the Ministry of Justice's Justice Data Lab gives organisations access to the government's administrative data on criminal reoffending, enabling research on specific questions about risks and rehabilitation (GovLab 2017b; MoJ 2018)

- in the United States, the California Policy Lab connects government agencies with academic researchers to answer specific policy questions using California's administrative data, such as how to reduce drug-related rule violations in the state's prisons (California Policy Lab nd; GovLab 2017a).

This cross-disciplinary data sharing and use is particularly suited to solving complex economic and social problems, such as those relating to the criminal and justice system per the above examples. The Commission has previously observed that supporting prisoner release via 'throughcare' — 'rehabilitation and reintegration aimed at helping inmates overcome a range of complex needs and return to society… coordinated to ensure offenders' needs are identified and the right supports are provided' (PC 2021a, p. 88) — would help to reduce reoffending rates. As the necessary supports span a range of government portfolios and community service providers (including in justice, healthcare, housing and employment services), sharing data between relevant agencies and private organisations would assist in implementing throughcare programs.

Finding 4.12
Data sharing between public and private sectors has productivity benefits

Collaboration between government and the private sector can lead to new opportunities for digitisation and data sharing, and derive more value from data provided to government agencies. Enabling government data sharing can benefit businesses and consumers by streamlining processes and improving service delivery, but only if data safety and security are maintained. The *Data Availability and Transparency Act 2022* (Cth) does not currently allow government data sharing with the private sector, which could prevent some high-value data uses.

Recommendation 4.3
Private sector access to government data

The Australian Government should enable government data to be securely shared with the private sector, so that not-for-profit organisations and businesses can undertake research and develop improved products and services for Australians.

This could be enabled by extending the *Data Availability and Transparency Act 2022* (Cth). Extension could be gradual, starting with accredited private organisations using the data for policy and research purposes to achieve social objectives, before being opened for accredited businesses to use the data commercially. Appropriate safeguards should be employed to ensure security and privacy concerns are addressed, and the government could consider utilising advances in technology for individual privacy preservation.

More value from data held by government-funded service providers

Opportunities for government-initiated data sharing extend beyond the data that is directly collected by government agencies. Governments fund various investments and services that generate potentially valuable data in their delivery. Even though much of this data is produced and held by service providers and users, data that is predominantly funded by taxpayers should be available for use in generating value for the community, subject to privacy and security protections.

Healthcare case study

Healthcare data is a good example of this, as the Australian Government provides significant subsidies for Medicare-funded health services and medicines on the Pharmaceutical Benefits Scheme. The potential productivity benefits of greater healthcare data sharing and use are well established, and can primarily be grouped into two categories (PC 2017a, pp. 522, 531):

- *improved service quality for the patient*. Sharing data between healthcare practitioners means that it is quicker and cheaper to access accurate medical records and transfer these between practitioners, leading to better healthcare decisions and reduction in low value care. Individual consumers recognise these benefits exist: the Consumer Policy Research Centre submitted that Australians 'largely want health care providers to have the information they need to provide quality care … 80% are ready to share their health data in a digitally enabled health system' (CPRC, sub. 115, p. 7)
- *more informed health policy, funding allocation and service delivery.* Policymakers, researchers and service providers would have access to more accurate population health data and be able to better measure health system outcomes. This could be used, for example, to improve the identification of the causes of disease and at risk populations. Greater visibility over outcomes could also inform the evaluation of various approaches to service delivery (and the efficiency and effectiveness of these), enabling improvements and funding decisions that would potentially help service providers to deliver quality care to more consumers.

Appropriate consideration should be given to the types of healthcare data that could be shared with and/or through government in order to achieve these benefits. For example, improving individual healthcare decisions and quality of care may require sharing data such as prescribed medicines and pathology test results, so that patients can experience relatively seamless care across different practitioners and avoid the need to repeat tests or risking prescription errors. In contrast, to achieve broader research and policy benefits, this type of patient-specific information is unlikely to be required. De-identified data about service use and outcomes linked across different parts of the health system (for instance, whether a patient who saw a GP was treated or had to subsequently engage with specialists or hospitals) might be more useful.

The benefits of data sharing must also be balanced against safety and privacy concerns. For example, even though the government provides significant funding for healthcare, their right to data from publicly funded health services may not include written medical records created by a practitioner. These are covered by both copyright and privacy laws, with patients having some rights to access the records. However, it is far from clear that government access to these records (at this time) would create social benefits that outweigh the costs — including the costs of practitioners potentially reducing the amount of useful information they include in these records.

The Australian Government's My Health Record (MHR) initiative is intended to provide a mechanism for collating, storing and sharing consumer health information (box 3.4). However, despite increased uptake over recent years, MHR is some way off from being a comprehensive source of information on all healthcare services used by a consumer. This, in turn, limits the benefits that can be achieved for both individuals and the community.

Interoperability between the data collection and storage systems of different healthcare providers and data users has been an ongoing barrier to MHR take-up, including in the aged care sector. For example, a 2021 survey of residential aged care providers by the Aged Care Industry Information Technology Council found that 71% used

software that does not interface with MHR (Health Metrics 2021). More broadly, the Commission observed in its *Innovations in Care for Chronic Health Conditions* report that 'many of the IT systems that GPs use are not interoperable with hospital IT systems, limiting communication and information sharing between these two sectors' (PC 2021b, p. 118). In an environment where caregivers and medical practitioners are often time poor, the additional time required to navigate systems that do not interface with other data sources — or to change their system to enable interoperability — can be a significant barrier to better data use.

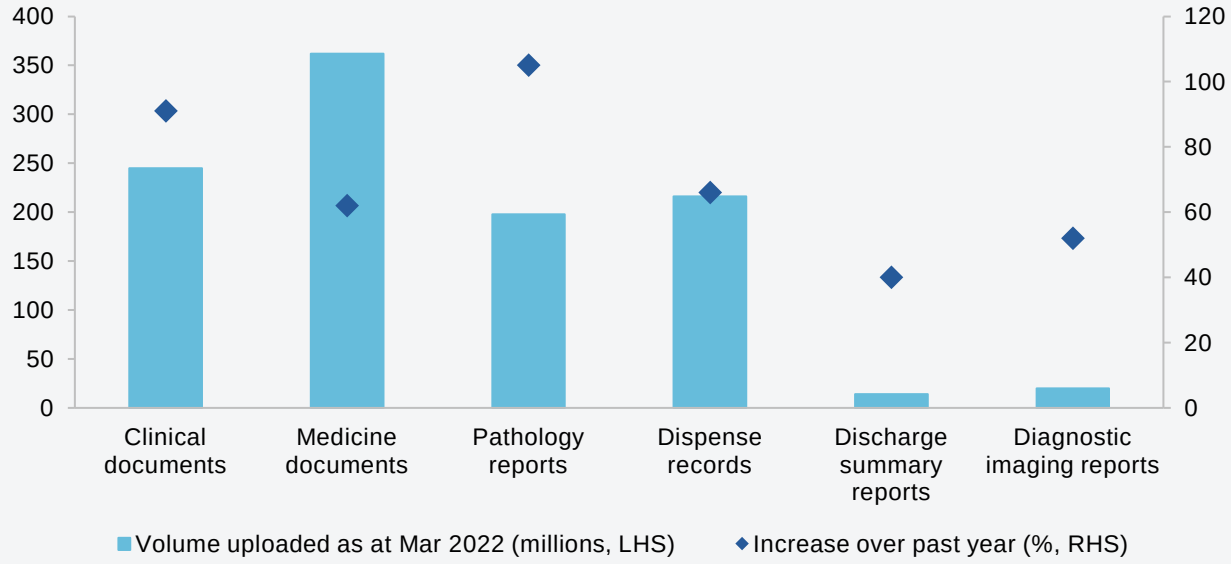
Box 3.4 – Use of My Health Record

The Australian Government introduced My Health Record (MHR) in July 2012 to improve consumer health data sharing. Initial uptake of MHR was slow, as it was opt-in until January 2019 and many medical practitioners and software providers were not well prepared to use MHR. In MHR's early years, slow uptake begat slow uptake as 'low usage throughout the healthcare system reduced the incentive for individual clinicians to use MHR. For example, patchy usage by [general practitioners (GPs)] meant that hospital staff saw little value in using MHR and vice versa' (PC 2021b, p. 119).

Since MHR was changed from opt in to opt out, the number of records with data has increased substantially, from 5.4 million people in January 2019 to more than 22.5 million in March 2022 (ADHA 2022). These records include 245 million clinical documents (such as those uploaded by hospitals, pathologists and radiologists) and 362 million medicine documents (such as those uploaded by GPs and pharmacists), with the volume of uploaded documents increasing by more than 50% over the past year for most document types (figure below). Early feedback from medical practitioners after the shift to an opt-out approach was mixed, with the Royal Australian College of GPs observing in July 2019: 'has Australia's digital health repository hit the threshold for usefulness? Some GPs give an emphatic yes, while others say it is still a work in progress' (Hendrie 2019). The continued growth of data stored in MHRs is likely to have increased its usefulness to consumers and service providers.

Data in My Health Record has increased significantly

Volume of documents uploaded by document type, March 2022



Source: ADHA (2022).

Box 3.4 – Use of My Health Record

However, despite the increased uptake, MHR is some way off from being a comprehensive source of data on all healthcare services used by a consumer. In addition to individuals being able to opt out, healthcare providers can also choose not to enter consumer data into a MHR, even if the individual has opted in. As such, the amount of detail contained within individual MHRs is variable; for example, although 99% of GPs are registered on the system, GPs report that one in 25 MHRs currently contain no data at all (Attwooll 2022).

Registration and usage is still low in parts of the system: as at March 2022, only 22% of specialists are registered on MHR and 10% have used it (ADHA 2022). And only 10% of residential aged care facilities were registered as at April 2021, with only 3% having used it (Cheu 2021). Given the potential benefits of consolidating health data for aged care residents, the Aged Care Royal Commission recommended 'universal adoption by the aged care sector of digital technology and My Health Record' by July 2022, including that all providers use a digital care management system that is interoperable with MHR (Pagone and Briggs 2021, p. 253).

There have been efforts to improve health data collection, sharing and interoperability outside of MHR.

- The Australian Government's Practice Incentives Program Quality Improvement (PIP QI) Incentive pays GPs up to $50 000 per year to collect and submit data about specific improvement measures to their local primary health network (PHN). The data is used to 'benefit patients directly at the practice level and to inform PHN regional planning and contribute to national health policy' (Department of Health 2019, p. 5). The Commission has previously reported 'mixed views from stakeholders on the PIP QI. Some considered it has encouraged practices to improve their data collection … However, others argued the data requirements were too low and would not lead to substantial improvements in quality of care' (PC 2021b, p. 150). The Practice Incentives Program also has a specific eHealth Incentive (ePIP), which rewards GPs that meet certain digital health requirements such as having an electronic secure messaging capability, sending the majority of their prescriptions electronically and using compliant software to participate in the MHR system (including uploading a minimum number of shared health summaries each quarter) (ADHA nd).
- Some states and territories have implemented health data initiatives in their own jurisdictions.
  - In Queensland, all referrals from GPs to public hospital specialists are made electronically through the Smart Referrals initiative, which was established under the 2016 *Specialist Outpatient Strategy* (Queensland Health 2016) to improve follow-up care, lower wait times and reduce human error. Digital referrals are integrated with existing GP software and can be tracked across the state.
  - In New South Wales, the Lumos program links GPs' primary care data with other health system data such as from emergency departments, hospital admitted patients, non-admitted patients and ambulances. It became a state-wide program in 2020 and, although not all GPs are on board, over 500 practices from across all 10 NSW PHNs are participating (NSW Health 2021).
  - In the Northern Territory, the Chronic Conditions Management Model requires all NT Health clinics to upload consumer data in electronic records. The data is cleaned and turned into automated reports that are provided back to practitioners to inform subsequent decisions about preventing and managing chronic health conditions (PC 2021b, pp. 123–124).
  - In Victoria, the Health Legislation Amendment (Information Sharing) Bill 2021 (Vic) seeks to establish a centralised electronic database for hospitals, ambulances and other healthcare providers to share patient data (Parliament of Victoria 2021). It would be mandatory for data to be shared in the database

(that is, patients are unable to opt out), which medical practitioners have noted is an important feature for generating benefits for patients and the broader system, and that 'the benefits outweigh the [privacy] risks' (Estcourt and Eddie 2022).

While these have improved data use, individual initiatives that only cover parts of the health system or particular jurisdictions are not sufficiently comprehensive or interoperable to result in increased service quality for all consumers, or enable more informed health policy development and resource allocation on a large scale. The Australian Healthcare and Hospitals Association submitted that past efforts to bring together primary healthcare data had similar limitations: 'in the absence of a national minimum dataset for primary healthcare, none [of the previous initiatives] have been comprehensively successful' (AHHA, sub. 27, att. 1, p. 16). And Bupa observed that to incentivise best practice in healthcare, 'we need to accelerate implementation of strategies for increased interoperability of health data. To improve service planning and outcomes it is essential that more data of higher quality is made available across both the public and private systems' (Bupa, sub. 69, p. 11).

Finding 4.13
Data from government-funded services could be better used

Much of the data generated by government-funded services and investments is not currently shared. But there could be large benefits resulting from better use of this data, subject to appropriate data security and privacy safeguards. For example, in health, data sharing can lead to improved services as providers have access to more accurate medical records and policymakers make more informed decisions.

Building on current foundations to improve health data sharing

The government should support more health data sharing, given the potential benefits that can be realised from greater use of this data and the significant policy levers that the government controls in funding and delivering health services. MHR could be a starting point for this — while it is currently not a complete source of health data on an individual patient (box 3.4), the underlying MHR infrastructure (including governance and security settings) can provide the foundation for a system in which data is shared more comprehensively and used to improve patient and sector-wide outcomes. Several government actions would encourage increased health data sharing using MHR, building on its current foundations.

First, there should be more clarity about opting out of MHR participation and what this entails for patients and practitioners. While patients have the right to opt out, the government should clarify that practitioners are required to upload relevant health information to MHR for patients who have not opted out of participating. The definition of 'relevant' information should be determined by government in consultation with patients and practitioners, and should be based on what information is most beneficial for informing patient care and enabling practitioners to improve health service delivery; for example, pathology and diagnostic imaging results and prescribed medications. Given that patients who have opted out of MHR could be missing out on significant improvements in the quality of the health services they receive, they should be required to confirm their decision to opt out each year after discussing with their GP.

Second, the government should support initiatives that make it easier for practitioners to upload information to MHR. Different healthcare practice management software has different functionality in how patient information can be entered and used, and not all software is integrated with the MHR system.

- In the short term, the government could publish a list of available software that can directly interface with MHR; for example, by allowing practitioners to automatically upload data to the MHR system when it is entered into a patient's record at the practice. This will enable practitioners to easily identify which software options could provide a more streamlined approach to interacting with MHR, and minimise unnecessary administrative burdens. The Australian Digital Health Agency (ADHA) already publishes a register of medical software products that conform with ePIP requirements (discussed above), including MHR-compatible software (ADHA 2021). This could be expanded to software that is used by other types of healthcare practitioners (as ePIP is a GP-only program), and with additional information about software features — the ATO's register of STP-compliant products, which is discussed above and includes details about each product's functionality and target market, could be a useful example to follow. Incentives to migrate to MHR-compliant software products could be considered for other healthcare practitioners beyond GPs, who can already benefit from ePIP.
- In the medium term, the government can address the broader interoperability issues in health data collection and storage (discussed above) by setting conformance standards for all medical practice software providers. These standards should require that practitioners can automatically upload relevant records to MHR via the software, and allow them to extract their patient data in an easy-to-use format to enable analysis at the practice level and transfer between software providers. The standards should also cover a consistent language and terminology, and a secure gateway to enable practitioners using different software to connect with each other. This could build on work already underway by the ADHA in developing 'terminology and information exchange standards to support the interoperability of digital health systems' (ADHA, sub. 145, p. 2).

Third, while MHR is already a secure environment for sharing patient data and is managed according to the Australian Government Protective Security Policy Framework, trust and confidence in the system can only be maintained if these security settings are continually monitored and updated. The government should review MHR's security measures on an ongoing basis to ensure that they remain fit for purpose in a rapidly evolving security threat environment.

The ultimate goal is to have a MHR system that allows comprehensive and seamless sharing of relevant health data between all practitioners that are providing care for an individual patient, as well as empowering patients by enabling them to access their own complete health record. Implementing the above steps would get some way towards this end goal: the benefits to patients and practitioners are significant, the system safeguards would be in place, and enhanced software functionality would reduce barriers to participation.

But there may be some practitioners that would still not be willing or able to upload patient information into MHR (for example, those that do not use practice management software and maintain paper records). This final 'tail' of practitioners may require some additional education and assistance and, as a last resort, compulsion to share relevant information for the benefit of their patients, particularly for service providers that receive government funding. For example, there have previously been suggestions that government could mandate that some health information be uploaded into MHR, ranging from pathology and diagnostic imaging results (Attwooll 2022) to patient outcomes and service provision data from all practitioners receiving government funding (AHHA, sub. 27, att. 1, p. 18). Given that buy-in from both practitioners and patients is an important factor underpinning use of and trust in MHR, mandating data sharing should be considered by the government as a last resort in weighing up the benefits and costs of system use.

The requirement to make healthcare data available to other practitioners and patients may change the nature of that data. Survey evidence from US mental health practitioners suggests that, when patients are given open access to their medical records through the OpenNotes software package, physicians change the tone and reduce the detail of their notes (Moll and Cajander 2020). And in Sweden, psychiatric care practitioners were found to be less candid with their notes (Petersson, Erlingsdóttir, and others 2018) and

oncology professionals noted changes to documentation practices, though this did not appear to have sizable negative effects on patient outcomes (Dobscha et al. 2016). Conversely, a review of empirical studies did not suggest that increased patient access to records through OpenNotes induced substantial changes to medical records (Blease, Torous and Hägglund 2020, p. 3). This indicates that the effect of more health data sharing on medical records (and patient outcomes) is, at best, unclear. However, as the requirement to share some healthcare data with patients may interact with documentation practices and therefore treatment (for example, where mental health records may themselves lead to patient trauma), there may be a small set of health records that require special conditions for sharing through MHR.

Finally, while the above discussion about implementation has focused on using MHR to improve service quality at an individual patient and practitioner level, the data in the MHR system could also be used to inform health policy and service planning, and disseminate best practice across the health sector. For example, data from primary care providers can help to 'facilitate increased efficiencies in care delivery, create more proactive preventive interventions, identify at-risk populations, inform health strategy and planning, support quality-improvement initiatives in Australian general practice and support judiciously targeted investment' (RACGP 2022, p. 19). The ADHA submitted that the size and quality of the MHR database means that 'it is a powerful resource to identify, support and monitor progress in vulnerable communities and cohorts … provid[ing] a more holistic view of patient's lives and support[ing] the identification of structural, social, economic, and cultural determinants of health' (ADHA, sub. 145, p. 6).

Using MHR to inform service planning and policy development would require a broader framework, as it is currently used for sharing individual patient records and the system's governance and safeguards are set up for that purpose. This would require extensive consultation with practitioners and the community on how the data could be de-identified and analysed for policy and planning purposes, in a way that maintains individual trust in MHR while also benefiting the broader system. For example, the Office of the Australian Information Commissioner has produced guidance on de-identification in collaboration with the CSIRO's Data61, and noted that 'appropriate de-identification may be complex, especially in relation to detailed datasets that may be disclosed widely and combined with other datasets' (OAIC, sub. 173, p. 5). Following the analysis, system-level benefits may then lead to further benefits at the individual practice and patient level, if the analysis was able to be fed back to the practice and re-linked to patients. This could involve retaining the linking identifier at the practice level to preserve anonymity in the system-level analysis.

Beyond healthcare

The rationales discussed for healthcare data apply more generally for increasing data sharing from other government-funded investments and services in sectors such as school education, childcare, aged care, criminal justice, community services and infrastructure contracts. In each case, the government would need to meet legitimate privacy and security concerns held by individuals and ensure that private data collection is not undesirably distorted by the data sharing initiative.

Large productivity and welfare gains could potentially result from better use of the data produced in each of these areas. As in the case of healthcare, these include benefits to individual consumers from improved service quality, and system-wide improvements arising from more informed resource allocation and research and policy development. One example of individual benefits is that sharing and linking service use data held by government-funded community services providers in areas such as housing and employment services could help to provide released prisoners with appropriate supports upon their return to the community. And at the system level, greater availability of data on childcare and education outcomes can help to inform policy decisions about funding allocation and effective service delivery.

Healthcare should therefore be only the starting point for the government in supporting more data sharing by government-funded service providers, to enable linked and seamless service delivery in other sectors. Depending on the sector and the existing (public and private) settings in place for collecting and using data, the government could play useful roles such as identifying relevant data to be shared and linked to benefit individuals, or setting technical standards for data sharing to promote interoperability — as suggested above in health. There may also be opportunities for government to use its funding levers to incentivise service providers to gather and share new data that could facilitate improved service delivery and productivity, such as data on service quality that is not currently collected.

Recommendation 4.4
Sharing data from government-funded services

The Australian Government should increase the safe sharing and use of data collected by government-funded service providers, including community, not-for-profit and private organisations. This would include identifying relevant data that could be safely shared and linked to benefit individuals receiving services, setting technical standards for data sharing to promote interoperability, and using funding levers to incentivise service providers to gather and share data that could improve service delivery and productivity.

Healthcare data should be targeted in the first instance to enable wellbeing benefits for individuals and productivity benefits at the practitioner and system levels. This could be implemented using My Health Record (MHR) as the foundation for a comprehensive data sharing system, and include provisions for:

- opting out of the system: Where consumers have not exercised their right to opt out of the system, practitioners should be required to upload agreed relevant health records to MHR. Patients that opt out should be required to confirm their decision each year after discussing with their general practitioner
- health software compatibility and standards: In the short term, the Australian Government should publish a register of health practice software that is integrated with MHR. In the medium term, it should set conformance standards that require all health practice software to be compatible with MHR to enable ready uploading of relevant records to MHR and extraction of patient data in an easy-to-use, secure and transferable format. The standards should also include consistent language and terminology, and a secure gateway to enable practitioners using different software to connect with each other
- de-identification to support system planning: The Australian Government should, in consultation with healthcare practitioners and the community, develop a framework for using the data in MHR in a de-identified way for health system-wide planning and policy development.

To support seamless service delivery, safe sharing of data held by government-funded service providers outside of healthcare — such as school education, childcare, aged care, criminal justice, community services and infrastructure contracts — should also be investigated and facilitated by the Australian Government.

3.3 Developing digital, data and cyber security skills

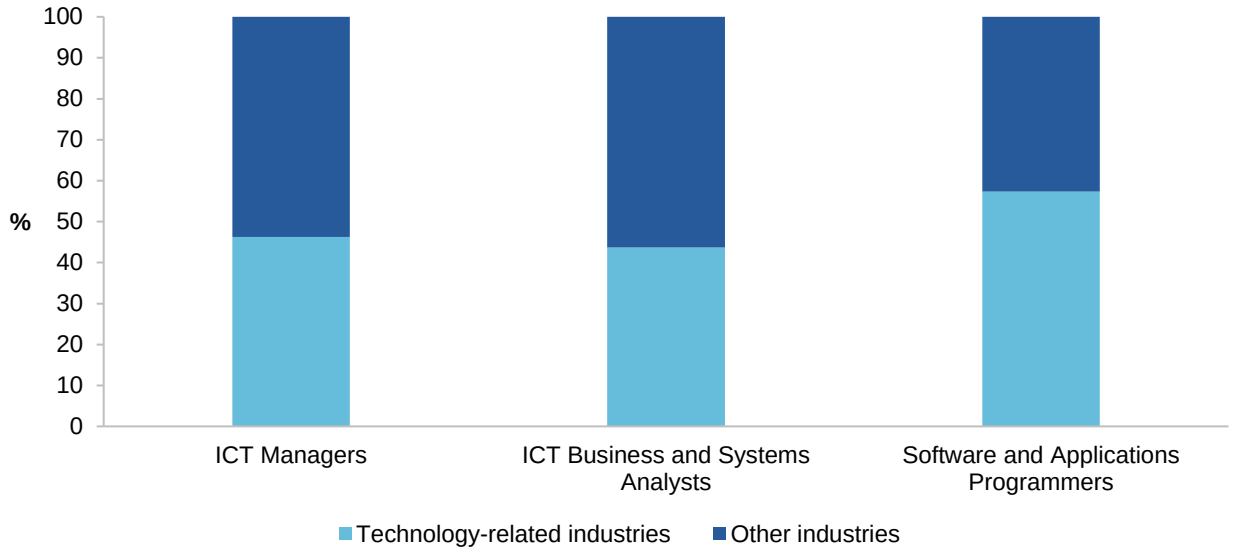
Demand for specialist digital and data workers is high across the Australian economy, not just in the technology sector, as ‘digital skills is one of the most important drivers of future prosperity’ (ATSE, sub. 8, p. 2). While the reported size of the ‘tech workforce’ in Australia varies depending on the occupations that are classified as working in digital and data-related roles, several industry associations have estimated that there are now over 800 000 workers employed in ‘tech jobs’ (ACS 2021a; TCA 2022). This includes highly

technical workers such as software developers and data scientists, as well as roles that support the adoption and experience of digital and data-related services by others (such as business analysts, technology product managers and user experience designers).

Many of these specialist workers are not employed by technology companies, or even consultancies that advise on digital and data solutions, but instead by businesses in other industries. For example, in the 2021 Census, less than half of all ICT managers and ICT business and systems analysts worked in the technology-related industries of information media and telecommunications or professional, scientific and technical services (figure 3.5). About 40% of software and applications programmers were employed outside these industries.

Figure 3.5 – Many technology workers are employed in other industries

Share of workers in selected ICT occupations employed in technology-related industries, 2021[a]



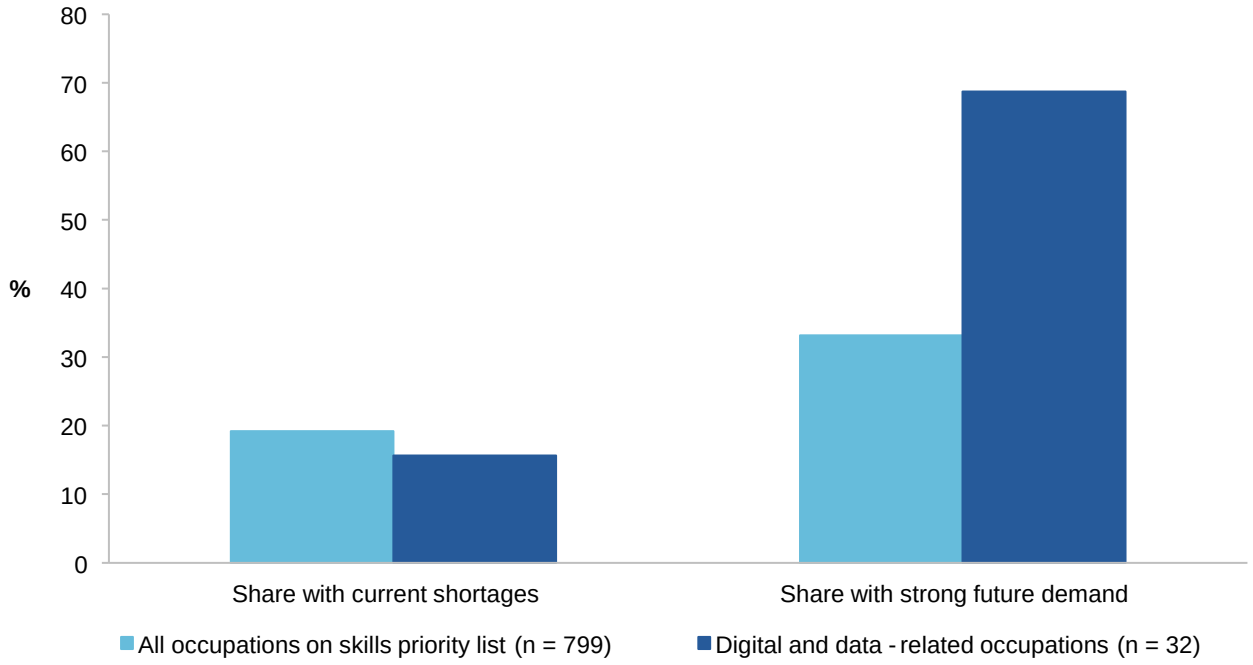
a. Technology-related industries are the 'information media and telecommunications' and 'professional, scientific and technical services' industries.

Source: ABS (*Population Census*, 2021).

As the Australian economy becomes increasingly digitised — a trend accelerated by the COVID-19 pandemic — demand for these specialist digital and data workers is expected to grow. In 2021, technology occupations on the then-National Skills Commission's (NSC's; now Jobs and Skills Australia) skills priority list were more than twice as likely to have 'strong' expected future demand in the next five years compared with the forecasts across all occupations on the list (figure 3.6). Industry also expects rapid growth in labour demand, with the Australian Computer Society forecasting that there will be demand for 1.2 million technology workers by 2035 (ACS 2021b, p. 6) and the Tech Council of Australia targeting technology employment of almost 1.3 million workers by 2030 (IA 2022a, p. 2).

Figure 3.6 – Strong future demand is projected for digital and data-related jobs

Share of occupations on the NSC's skills priority list with high current and future demand, June 2021[a,b]



a. The skills priority list includes occupations at the 6-digit ANZSCO level. The 32 occupations included as digital and data related are: Chief Information Officer, ICT Project Manager, ICT Trainer, ICT Account Manager, ICT Business Development Manager, ICT Sales Representative, ICT Business Analyst, Systems Analyst, Multimedia Specialist, Web Developer, Analyst Programmer, Developer Programmer, Software Engineer, Software Tester, Database Administrator, ICT Security Specialist, Systems Administrator, Computer Network and Systems Engineer, Network Administrator, Network Analyst, ICT Quality Assurance Engineer, ICT Support Engineer, ICT Systems Test Engineer, Telecommunications Engineer, Telecommunications Network Engineer, Hardware Technician, ICT Customer Support Officer, Web Administrator, Radiocommunications Technician, Telecommunications Field Engineer, Telecommunications Network Planner, and Telecommunications Technical Officer or Technologist. **b.** Future demand is based on the NSC's five-year employment projections, which combine forecasts from autoregressive integrated moving average and exponential smoothing with damped trend models, with known future industry developments and other NSC research.

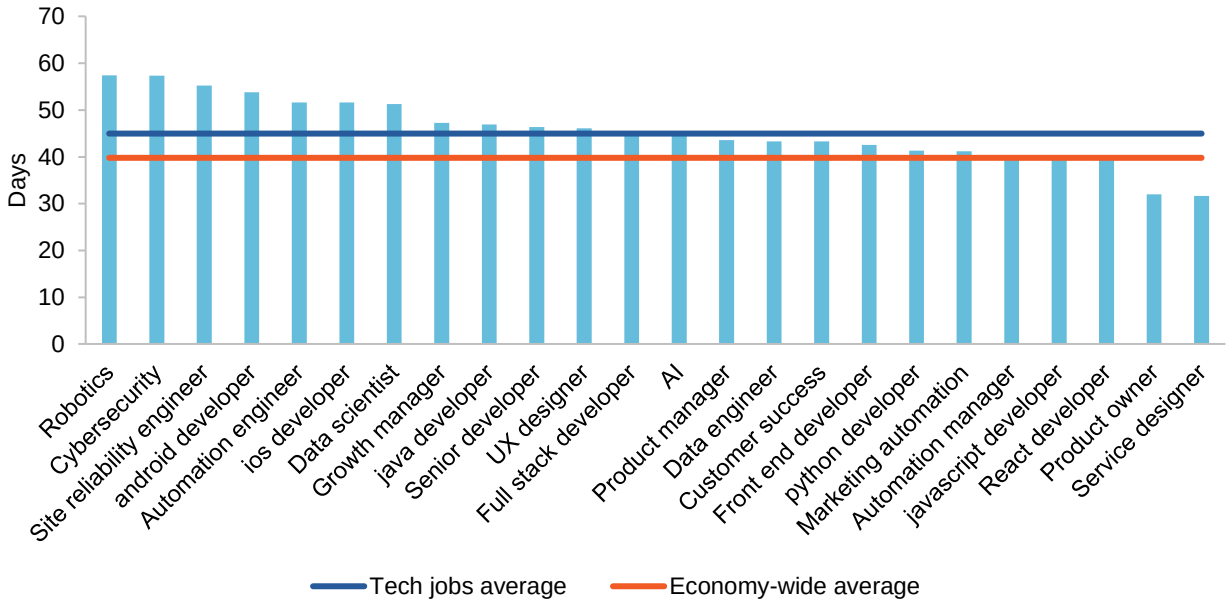
Source: NSC (2021a).

The skills priority list reported that the share of technology occupations in current shortage was broadly similar to the overall list in 2021. Analysis by the Tech Council of Australia using job ads data from Indeed, an online job search platform, suggests that the average age of open technology job ads (at 45 days) is higher than the economy-wide average (40 days). There are some particularly specialised roles that take longer to fill — such as in robotics, cyber security and niche engineering and developer roles (figure 3.7). In stakeholder engagement undertaken by the NSC, employers experiencing current challenges hiring relevant digital and data skills stated that:

> …where there was recruitment difficulty, this was experienced nationally, and that particular difficulty was experienced recruiting for experienced positions. Reported recruitment difficulty was most often attributed to the lack of technical skills or qualification of applicants, a lack of suitable or experienced applicants, or the specialised nature of roles. … The most frequently mentioned challenge facing recruitment in these occupations in the future is the lack of a locally trained workforce. (NSC 2021b, p. 5)

Figure 3.7 – Specialist digital and data roles take longer than average to fill

Weighted average age of open job ads, 30 September–1 October 2021[a]



a. This analysis by the Tech Council of Australia used job ads data from online job search platform Indeed. The number of open ads was collected for each job and segmented based on days since posting (7, 28, 56, 84, 102, 130 day buckets). The weighted average age was calculated by multiplying the share of job ads open within a particular time bucket by the midpoint between the minimum and maximum days of that bucket.

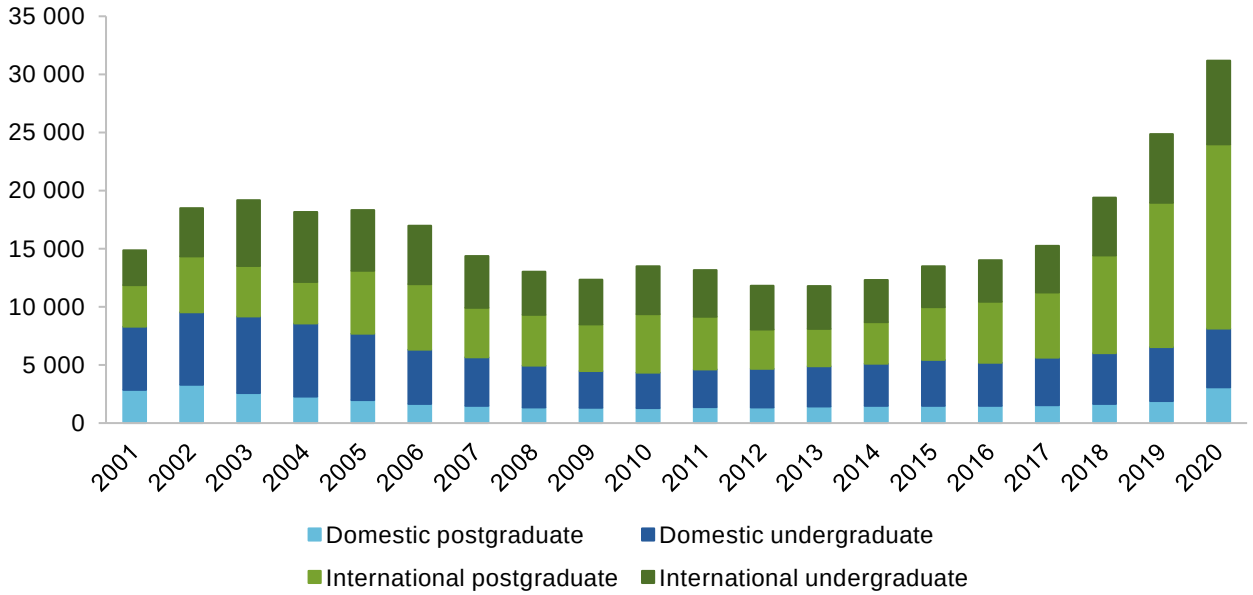
Source: Tech Council of Australia (pers. comm., 31 May 2022).

Specialist digital and data skills from formal education and training

Universities provide one pathway for digital and data skills development, and information technology (IT) degree completions have steadily increased over the past decade, rising particularly strongly in recent years (figure 3.8). While IT degree completions have increased for both domestic and international students, the latter group experienced significantly faster growth, with an average annual growth rate of 27% between 2016 and 2020 (compared with 12% for domestic students). As the latest available data on university degree completions predates the greatest disruptions caused by COVID-19, the pandemic's total impact on IT degree completions by international students remains to be seen.

Figure 3.8 – IT university degree completions have increased over the past decade

IT university degree completions by qualification level and citizenship category, 2001 to 2020[a]



a. The Department of Education, Skills and Employment changed the format of its completions data publication in 2020. Completions data for 2016 to 2020 is from the Award Course Completions Pivot Table, while data for 2001 to 2015 is from the Higher Education Data Cube (uCube).

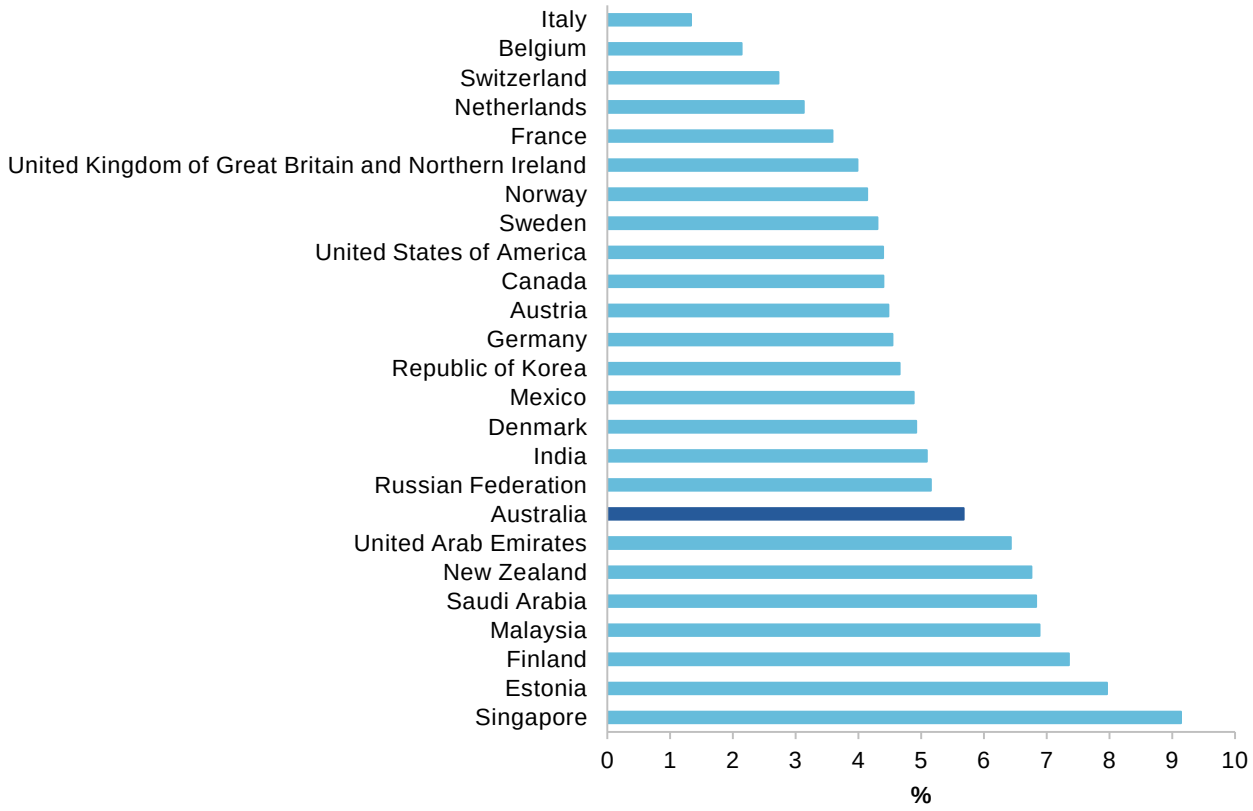
Source: DESE (2021, 2022).

The share of IT university graduates in Australia is relatively high compared with many other countries, with 6% of tertiary education graduates completing studies in information and communication technologies — higher than in the United States, United Kingdom, Canada and various European countries (figure 3.9). However, this does not necessarily translate to a larger pipeline of specialist digital and data workers in Australia. Industry stakeholders observe that 'approximately 1 in 2 of these international [IT] students do not permanently migrate to Australia, which means that our high enrolments overstate the impact that Australia's universities have on training our tech workforce' (TCA 2022, p. 5).

There have been approximately 20 000 annual completions of IT programs in the vocational education and training (VET) sector in recent years, with a growing share of these being international students (up from 10% in 2016 to 28% in 2020; figure 3.10). Post-study outcomes for students completing IT VET programs are relatively poor — in 2021, 73% reported that they were employed or in further study after completing their IT VET course, compared with 86% across all fields of education (NCVER 2022). However, students who are able to find employment in the technology sector after their VET studies perform relatively well, with the average wage gap between a VET qualification and a bachelor's degree being only 3% for entry-level roles, compared with 15–17% for entry-level workers in alternative industries (TCA 2022, p. 10).

Figure 3.9 – Australia has a relatively high share of ICT graduates

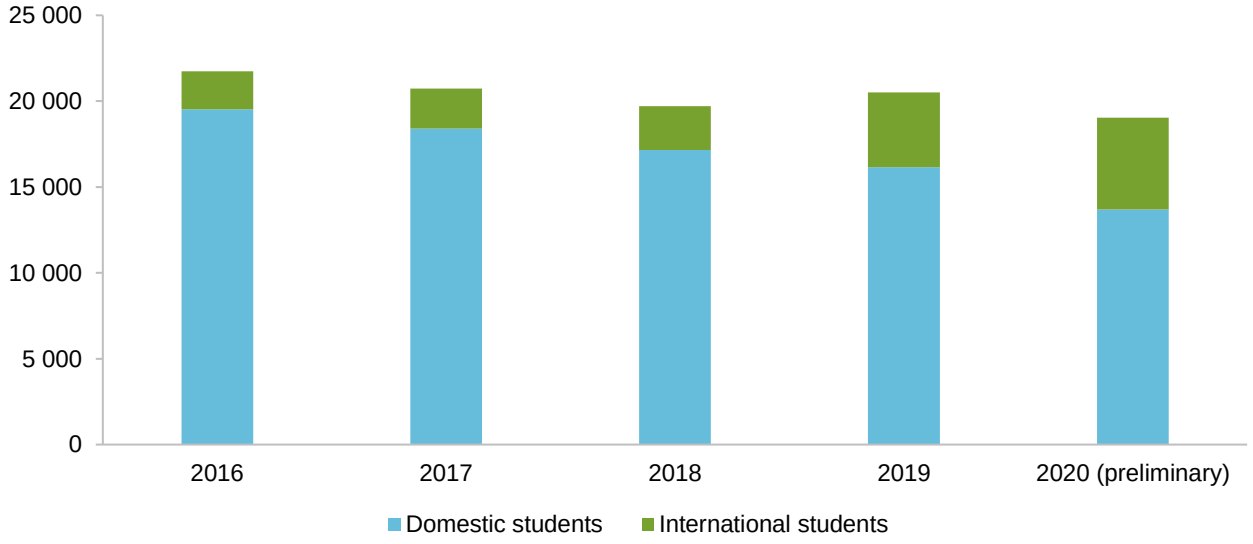
Share of tertiary education graduates graduating from ICT programmes, 2019



Source: UNESCO (2021).

Figure 3.10 – Domestic IT VET program completions have declined, while international completions have increased

VET completions in the IT field of education by citizenship category, 2016 to 2020



Source: NCVER (2022).

Short courses for digital and data reskilling and upskilling

Not everyone seeking employment in technical digital or data roles wants to complete an undergraduate or postgraduate degree — for example, individuals who are already in the workforce might want to transition into a specialist technology job from an adjacent role, without spending years returning to study. Other, more flexible, methods for upskilling or reskilling are required so that these workers can fill gaps in their technical knowledge while continuing to utilise relevant capabilities developed through their prior work experience. The Tech Council of Australia has stated that 'reskilling and upskilling workers must become the primary way tech jobs are filled' in order to meet future demand for specialist technology workers (TCA 2021b, p. 3).

There are a range of reskilling and upskilling options available for workers to develop the specialist digital or data capabilities required to transition into a technical role. Alternatives to a formal full-length qualification are offered by various organisations, and enable workers to 'obtain targeted skills or knowledge in a shorter timeframe and at a reduced cost relative to traditional tertiary education' (ACS 2020, p. 35).

- Vendor certifications are provided by companies that offer software or data services to train users of those services. Examples include Cisco's certifications across a range of technology categories (such as security, enterprise and DevNet) and levels (from entry level up to expert) (Cisco 2022); Microsoft's 200+ certifications in areas such as its Azure cloud services and security solutions (Microsoft 2022); and Amazon's certifications ranging from foundational Amazon Web Services cloud knowledge through to specialty domains in machine learning, advanced networking and databases (AWS 2022).
- Tertiary education institutions have set up separate entities that offer short courses targeted at developing specific digital and data skills. For example, RMIT Online has 6–16 week online courses to develop technical skills such as AI programming, app design and data analytics (RMIT 2022).
- Various learning platforms offer shorter courses for workers to develop technical skills. For instance:
  - Some companies deliver their own education and training courses in specialist digital and data capabilities, such as General Assembly's immersive courses in software engineering, data science and user experience (General Assembly 2022) and Academy Xi's online courses in digital product management, web development and data analytics (Academy Xi 2022)
  - Online education providers are collaborating with companies to offer new training options. For example, Google has partnered with Coursera to launch three professional certificates in data analytics, project management and user experience design, while Microsoft and General Assembly have a partnership to develop scalable AI training solutions (Coursera 2021; Microsoft 2019). Outside of big technology companies, Udacity has worked with AT&T and Shell to create tailored courses in 'hard-to-source, in-demand skills sets' such as web development and data science (AT&T) and artificial intelligence (Shell) (WEF 2020b, p. 48).

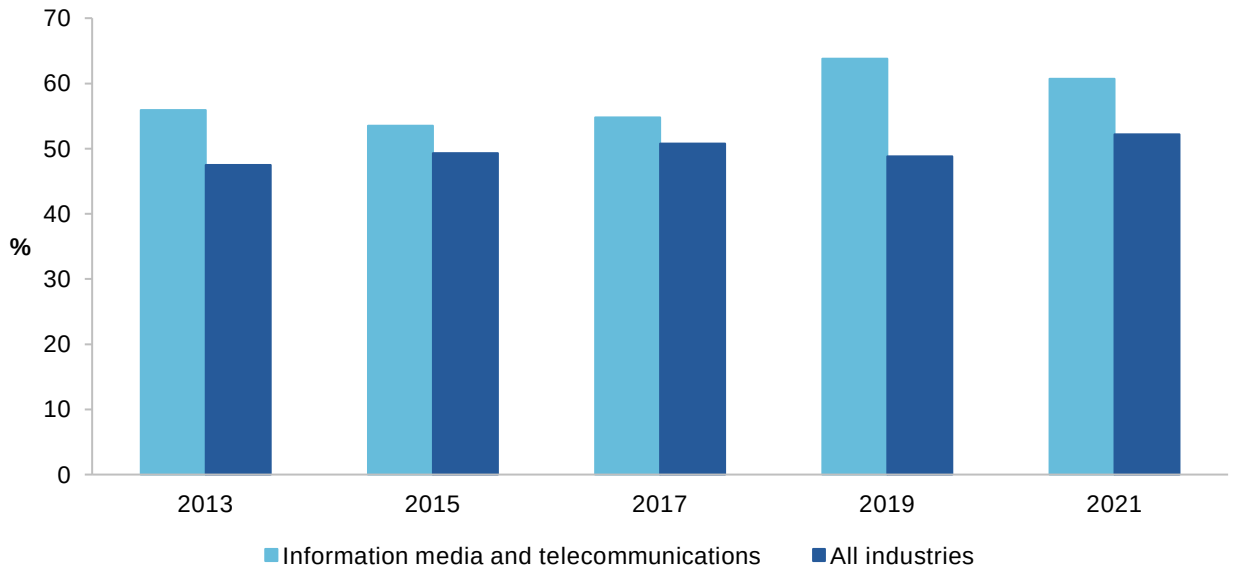
Women are more likely than men to enter the tech workforce through a reskilling pathway, by moving from another sector into a specialist technology role in their early to mid-career (TCA 2022, p. 5). In contrast, men are more likely to enter the tech workforce directly from education or training at the start of their career, and then move jobs within the sector. Greater use of these shorter and more flexible learning options to develop technical digital and data skills could therefore help to lift female participation in specialist technology roles, as only 1 in 4 workers in Australia's tech sector are women (TCA 2022, p. 1).

Employers with digital and data skill needs can also prefer shorter-form learning options offered by industry providers, compared with the formal qualifications delivered by universities and the VET sector. Industry-delivered training — such as vendor certifications — are viewed by some employers as developing more relevant skills than the formal education system: employers state that these vendor training options are '"focused and tailored", "cutting edge", "very relevant", "highly flexible" [and] "great value for money"' (Bowman and Callan 2021, p. 46). Shorter-form learning options could be particularly useful for SMEs — which are more likely to cite lack of skills as a barrier to technology adoption (section 2.1) — to build digital and data capabilities, as the financial and time costs of training are relatively high for these employers (OECD 2021, p. 10).

Surveys of IT industry employers routinely find that they are more likely to use unaccredited training than the average use across all industries (figure 3.11). And in 2021, 83% of employers in the information, media and telecommunications industry that used unaccredited training reported satisfaction with training to meet their skill needs, compared with only 58% of employers using nationally recognised training (NCVER 2021).

Figure 3.11 – Employers in the IT industry are more likely to use unaccredited training

Share of employers using unaccredited training in the past 12 months by industry, 2013 to 2021



Source: NCVER (2021).

The private benefits associated with these training options means that many are already being taken up by Australian workers and businesses. In addition to the private benefits, some governments have also introduced initiatives aimed at encouraging workers to upskill and reskill in digital and data using short training courses. For example, Victoria's Digital Jobs program supports 5000 mid-career employees to undertake 12 weeks of industry-backed training, followed by 12 weeks of work experience in a digital role (DJPR 2022). At the national level, the Digital Skills Organisation launched a pilot project to train 100 data analysts, with participants undertaking short unaccredited training tailored to employers' needs on digital and data skills, and funding incentives tied to training completion and employment outcomes (DSO 2021).

Several inquiry participants suggested that the government should provide further financial incentives for digital and data-related short courses — such as micro-credentials and 'boot camps'— for upskilling and reskilling purposes (for example, Australian Investment Council, sub. 83, p. 7; BSA, sub. 134, p. 5; Engineers Australia, sub. 85, p. 14; UTS, sub. 92, p. 2). Government support for these types of courses and

lifelong learning among Australian workers more generally is discussed in the inquiry's companion volume *From learning to growth*, which recommends that the government could encourage uptake by trialling targeted policies for work-related upskilling and reskilling, and extending self-education tax deductions to education that is likely to lead to income outside of current employment. Existing programs designed to support lifelong learning, such as Employability Skills Training and the incoming Skills and Training Boost, should also be evaluated for their effectiveness at facilitating additional training.

Shorter-form and unaccredited training will not always be the most suitable option for workers looking to reskill or upskill into a technical digital or data role. RMIT Online, a provider of both short courses and full-length qualifications in various specialist digital and data areas, notes that 'while short-term training may be enough in many cases, if people are looking for a career change or a brand new, complex skillset, longer-term and structured education by a tertiary institution may be needed' (RMIT Online and Deloitte Access Economics 2021, p. 25). The most efficient channel for reskilling or upskilling will depend on an individual's previous education and work experience and the skills that need to be developed in transitioning to a new technical role.

Finding 4.14
Shorter-form learning options help develop digital and data skills

Short courses and unaccredited training can be preferred for developing digital and data skills, as they are often more relevant and flexible. Businesses and workers are already using options such as industry-delivered vendor certifications to upskill and reskill, and government support (such as through tax incentives) could further increase uptake where policies are targeted and evaluated for additionality.

Supplementing the local workforce with overseas experience

Not all skills gaps in specialist digital and data capabilities can be filled through education and training. The then-National Skills Commissioner previously stated that there can be a range of factors that result in demand exceeding supply for specific skills, particularly in the short term, including employers desiring:

> … on the job experience, things that are difficult to provide through formal training alone; [or] a highly technical or specialised skill which is emerging and hence might not yet be reflected in the training system. (Boyton 2022)

Various advanced technical skills in the digital and data space are likely to fit this description. For example, technology product managers — who combine business, technical and user experience skills to oversee a product's development in a way that meets customers' needs — for large-scale products are difficult to find in Australia. Industry stakeholders report that people who have the capabilities to manage products at scale learn by doing. With a relatively small (though growing) number of technology companies operating at a large enough scale in Australia, there is a relatively small talent pool to meet employers' demand for experienced product managers in the short term. Some have noted that 'if Australia wants to improve its technology industry, the discipline of product management "needs to grow up a little bit"' (Gillezeau 2020).

Because of the importance of on-the-job experience in developing these types of specialised skillsets, many employers look to recruit workers from overseas where there is a deeper talent pool. This targeted sourcing of workers from overseas is used not only to fill immediate skills gaps, but also to support the longer-term development of the workforce in Australia. For example, overseas workers join local teams and are able to bring their experience to support on-the-job learning for local employees. As technology products are scaled up, these local workers can further develop more advanced technical skills on the job.

Some businesses operating internationally have work-from-anywhere policies, which enable them to hire specialist digital and data workers in other countries and integrate them with their Australian teams. This distributed workforce approach has increased through the COVID-19 pandemic; for example, Atlassian introduced its 'Team Anywhere' policy in 2020 and transitioned to a fully distributed workforce (Atlassian 2022). The Commission heard from both large and small Australia-based technology companies that they are able to tap into overseas skilled workers by building integrated teams comprised of local staff and employees in North and South America, Europe, Asia and Africa.

Skilled migration is another channel for Australia-based businesses to access the global talent pool for specialist digital and data skills. There are several options for overseas workers with these skills to acquire a visa for employment in Australia.

- The Temporary Skill Shortage (TSS) visa (subclass 482) is 'important for technology companies of all sizes' (TCA 2021a) as a source of workers with advanced technical skills that are difficult to recruit in Australia. It includes short and medium-term streams that require workers to be sponsored by an employer for an occupation that is on a relevant skilled occupation list (Home Affairs 2021d). As at end February 2022, specialist digital and data occupations eligible for the short-term stream included software testers and web developers, and eligible workers for the medium-term stream included developer programmers and software engineers (Home Affairs 2021c).
- The Global Talent (Independent) visa (subclass 858) seeks to attract highly skilled workers across ten target sectors, including 'DigiTech', 'Agri-food and AgTech' and 'Financial Services and FinTech'. These respectively represented 34%, 12% and 1% of the 9 584 visas issued in 2020-21 (Home Affairs 2021a, p. 37). There are 15 000 visa places available under this program in 2021-22 and workers do not need to be employer sponsored (Home Affairs 2021f).
- The Global Talent (Employer Sponsored) program allows employers to sponsor workers with specialised skills that are not eligible for other visas (such as the short and medium-term streams of the TSS visa). Visas are issued under the labour agreement stream of the TSS visa and accredited employers are not restricted to occupation lists (Home Affairs 2021e). Several technology and data-related employers were accredited as at end February 2022, including Amazon, Culture Amp and Refinitiv (Home Affairs 2022b).

Several stakeholder submissions noted that the approach of using skilled occupation lists for some of these visas could be improved, as this would better enable employers to address local digital and data skills needs (AIC, sub. 71, p. 11; Consult Australia, sub. 28, p. 9; TCA, sub. 51, p. 16). In particular, the Tech Council of Australia observed that 'Australia's skilled occupation list is arbitrarily complex and outmoded, due to its reliance on an occupation classification system that does not recognise tech sector roles' (TCA, sub. 51, p. 16). Some inquiry participants suggested that the government should review skilled migration policy settings to better attract and prioritise workers with the digital and data skills that are currently in high demand across Australian employers (ACCI, sub. 175, p. 13; CPRC, sub. 115, p. 8).

The companion volume in this inquiry, *A more productive labour market*, discusses migration policy more generally and includes several recommendations to improve Australia's skilled migration program, such as shifting away from overly restrictive and inflexible occupation lists for employer-sponsored temporary and permanent skilled migration. Instead, the government should implement wage thresholds for employer-sponsored visas, whereby employers can sponsor overseas workers in any occupation as long as they are paid above the relevant threshold (with a lower threshold for temporary migration and permanent migration thresholds to increase with age). Implementing such changes would improve the ability of Australian employers to supplement their workforce with specialist digital and data skills from overseas that are difficult to source or develop locally in the short run.

Finding 4.15
Skilled migration assists in meeting digital and data skills needs

Not all digital and data skills needs can be met locally or with education and training in the short term. Skilled migration enables businesses to access a deeper talent pool, particularly for specialist skills that are difficult to find or develop in Australia. However, the occupation lists that underpin much of the skilled migration system are not sufficiently flexible or up-to-date to meet employers' digital and data skills needs.

Increasing digital literacy among the broader population

In addition to the specialist technology and data workers that are in high demand, an increasingly digitised economy and society — as discussed in section 1.1 — means that most Australians need some level of baseline digital skills (sometimes referred to as 'digital literacy') in order to work and live. The Australian Government's *Digital Economy Strategy 2030* reported that 87% of jobs now require digital skills – across every sector and industry (PMC 2021c, p. 16). The Smith Family has observed that a lack of basic digital skills in some population cohorts has flow on effects to their ability to participate in a high-skilled 21st century economy (The Smith Family, sub. 26, p. 15).

In this context, ensuring that the broader population has adequate levels of digital literacy supports both a more productive workforce and a more inclusive society, as services and other interactions continue to move online. Increasing broader digital literacy may also serve to raise awareness of cyber security risks and lessen the impact of cyber attacks.

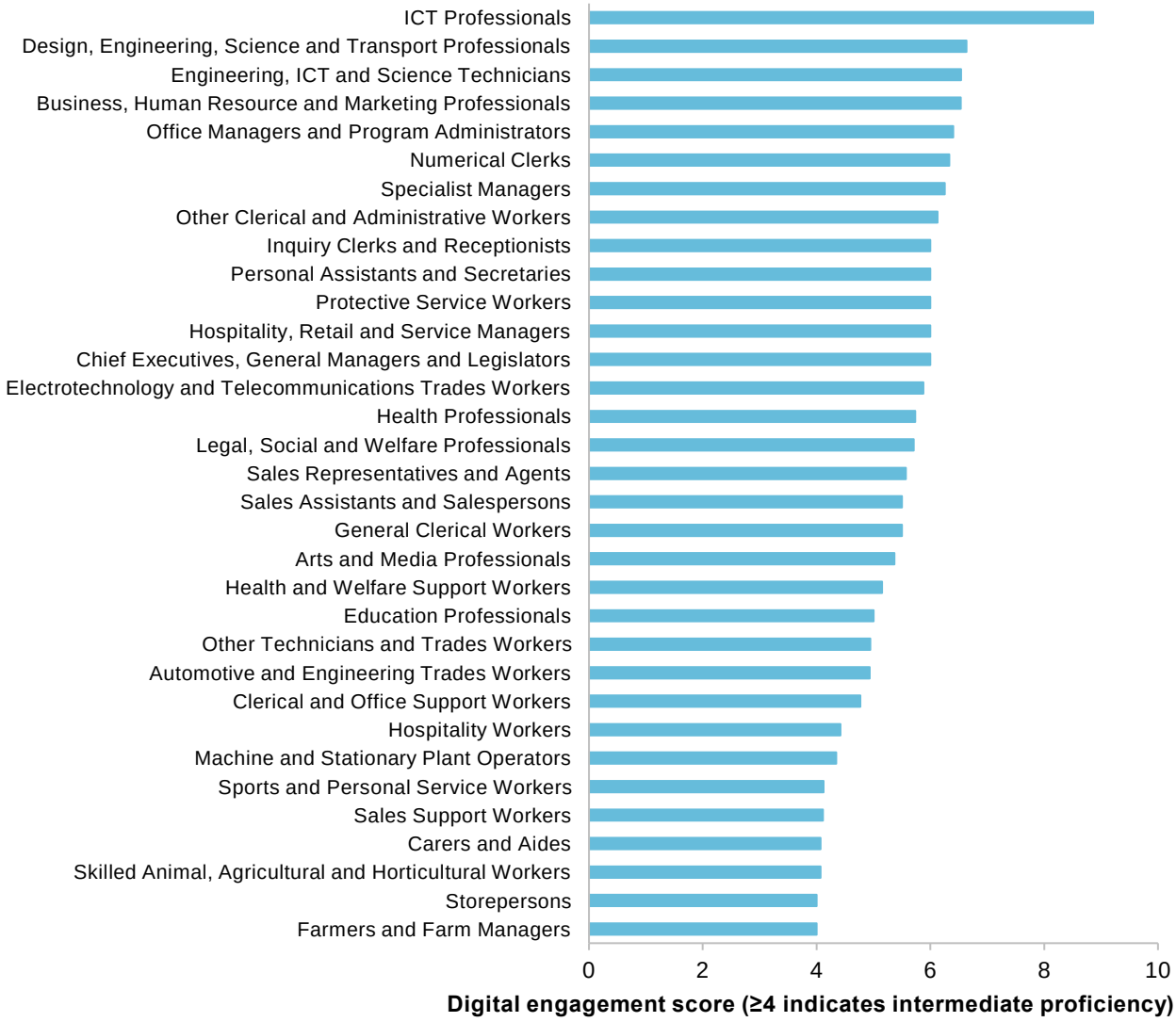
The jobs that require a good foundation of digital literacy are many and varied. According to the NSC's Australian Skills Classification, most occupations in the Australian labour market need either intermediate or high proficiency on the digital engagement core competency (which provides an indication of the digital literacy requirements of different jobs).[17] This extends beyond IT roles, with other occupations requiring relatively high competency in digital engagement including engineering and science professionals, business and marketing professionals, and office managers (figure 3.12).

However, there are concerns about digital literacy levels among Australian employers and employees. From an employer perspective, recent research on the learning and development activities of Australian businesses found that 26% of surveyed businesses reported digital literacy as a key skills gap (increasing to 34% for the business services industry) (DeakinCo and Deloitte Access Economics 2022, p. 11). And a survey of Australian workers found that with regards to digital literacy skills, 24% of those surveyed stated that they 'don't have the skill level required [by their employer] or skill is out of date' (RMIT Online and Deloitte Access Economics 2021, p. 15). Digital literacy was the second-largest skills gap reported by workers, with data analysis being the biggest identified gap — inadequate or outdated data analysis skills were reported by 30% of those surveyed (RMIT Online and Deloitte Access Economics 2021, pp. 14–15).

[17] The Australian Skills Classification contains '10 core competencies common to every occupation in Australia [and] uses a 10-point scale to describe the complexity of each core competency for each occupation' (NSC nd). The digital engagement core competency captures non-specialist skills associated with using technology — including hardware and software — in any occupation. Occupations are assessed as requiring digital engagement proficiency of basic (score of 1–3; for example, sending simple email communication), intermediate (score of 4–7; for example, using software on a portable device) or high (score of 8–10; for example, setting up a large computer system).

Figure 3.12 – Digital competency is required for many occupations outside of IT jobs

Average score on digital engagement competency for 2-digit occupations requiring intermediate proficiency or higher, March 2022[a]



a. The NSC's Australian Skills Classification contains a competency score on digital engagement for 799 selected 4- and 6-digit occupations (as defined in ANZSCO). Scores corresponding to occupations within a given 2-digit grouping have been averaged for this figure. Only occupations requiring 'intermediate' or higher proficiency (that is, scoring four or more on the 10-point scale) are depicted in this figure, which represents 33 of the 43 2-digit occupation groupings.

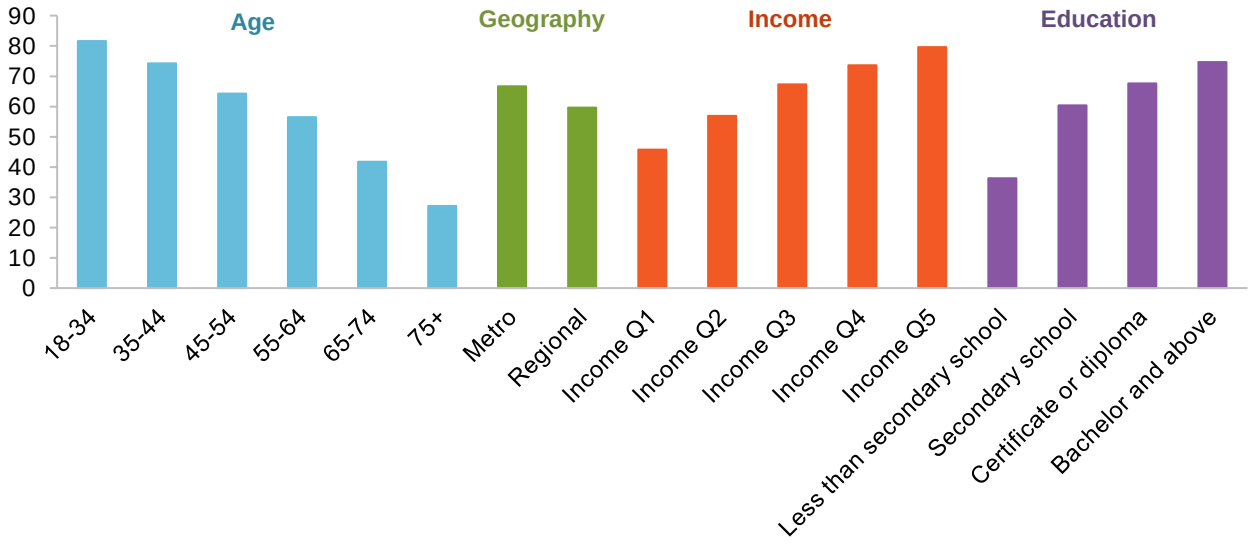
Source: NSC (2022).

Some segments of the Australian population have lower digital literacy levels than others. For example, the Australian Digital Inclusion Index reported a significant gap in digital ability between older and younger Australians in 2021 (figure 3.13). The Index is based on the Internet Skills Scale, which includes both basic and advanced digital capabilities; advanced capabilities (such as operating IoT technologies and using the cloud) may go beyond the baseline skills required to undertake everyday digital tasks. However, even when only considering basic operational skills (such as downloading files and setting passwords) and information navigation (such as searching the internet and verifying information), there are substantial gaps between the youngest and oldest age cohorts (ADII 2021). The Index also reports a digital ability gap between Australians

living in metropolitan and regional Australia, and lower digital ability scores for cohorts with lower income and education levels (figure 3.13).

Figure 3.13 – Digital ability declines with age, income and education levels and is also lower in regional Australia

Index of digital ability overall in 2021, by age, geography, income and education[a]



a. Income quintiles are defined as follows: Q1 represents incomes less than $33 800, Q2 represents $33 800 to $51 999, Q3 represents $52 000 to $90 999, Q4 represents $91 000 to $155 999, Q5 represents incomes of $156 000 or more.

Source: ADII (2022).

As increasing amounts of economic and social activity are taking place via online channels, low digital literacy in some population cohorts can reduce their ability to consume essential services and undertake everyday transactions. Just as a lack of regional digital infrastructure may lead to social exclusion (section 3.1), people with limited digital ability can face difficulties accessing services such as home schooling, telehealth consultations and online banking. This could compound economic and social disadvantage; for example, low digital literacy among low income earners or those who have had limited education opportunities can be a significant barrier to accessing and maintaining employment (ACOSS 2016, p. 3). And limited ability to use digital health services in remote areas, which already have greater difficulties accessing health care in person, can lead to more vulnerabilities and health risks in these areas (Beaunoyer, Dupéré and Guitton 2020).

There are already government initiatives aimed at improving the digital literacy of various cohorts. For example, the Australian Government's Regional Tech Hub — delivered by the National Farmers' Federation and Australian Communications Consumer Action Network — supports regional and remote Australians to connect to new technologies, including by 'troubleshoot[ing] common connectivity problems' (DITRDC 2019). The Victorian Government's Regional Digital Fund provides grants that include projects for building digital skills and capability in regional Victoria (RDV 2021). And to increase the digital literacy and online safety of older Australians, the Australian Government's *Be Connected* program provides a range of resources and interactive tools, including personalised mentoring in local community settings (DSS 2021).

3.4 Balancing cyber security and growth

The growing number of cyber attacks in Australia and the increasing sophistication of these attacks have negative economic consequences (section 2.2). The government's role in mitigating and managing cyber risk is important, but can involve restrictions or additional requirements on private entities, which may inhibit economic growth. For example, unnecessarily burdensome regulation can divert businesses' resources away from other operations, which may negatively affect broader business activities or undermine existing security protocols. The Australian Institute of Company Directors has stated that:

> There is a risk that [an overly compliance-focused] approach will divert attention from senior management and directors in actively responding to cybersecurity threats and building resilience and ultimately add to the existing regulatory burden with negative productivity results. (AICD, sub. 44, p. 7)

As such, government activity in the cyber security policy area should be measured and carefully balance the costs of any intervention against its benefits.

Governments should support both cyber resilience and response to cyber attacks. The World Economic Forum defines cyber resilience as 'not only defending against cyberattacks, but also preparing for swift and timely incident response and recovery when an attack does occur…[and] the ability of an organization to transcend… any stresses, failures, hazards and threats to its cyber resources within the organization and its ecosystem' (WEF 2022, p. 15). Although this indicates that cyber resilience is broader than just the attack response itself — as it includes elements of prevention beforehand and longer-term recovery after the fact — many stakeholders focus narrowly on responding to an attack. A recent global survey of cyber leaders found that 59% did not have a good understanding of the differences between cyber security response and cyber resilience, believing that the two are synonymous (WEF 2022, p. 15).

There is already significant Australian Government activity addressing cyber security issues. *Australia's Cyber Security Strategy* was released in 2020 (Home Affairs 2020a), building on an earlier strategy from 2016, and various pieces of legislation and initiatives have been implemented (box 3.5).

Box 3.5 – Australian Government activity on cyber security issues

The centrepiece of the Australian Government's cyber security policy is *Australia's Cyber Security Strategy 2020*, which highlighted a range of investments made by the government's $1.67 billion of (then) budgeted expenditure on cyber security over 10 years (Home Affairs 2020a). This included the Cyber Enhanced Situational Awareness and Response package, which was announced in June 2020 and allocated funding to various initiatives such as expanded capabilities and workforce at the Australian Signals Directorate (ASD), creating a new cyber threat-sharing platform for information sharing between industry and government, and more research, mitigation and prevention activity (Defence 2020). The Australian government also released the *National Plan to Combat Cybercrime* in March 2022 to increase collaboration between Commonwealth, state and territory partners in combating cyber crime (PMC 2022b, p. 17).

The Australian Cyber Security Centre (ACSC) is part of the ASD and was established in 2014. It monitors cyber threats, provides information about good security practices, and investigates and assists with responses to security incidents. The ACSC runs various programs to improve cyber security across both large critical infrastructure organisations and smaller businesses and individuals. It also promotes

Box 3.5 – Australian Government activity on cyber security issues

collaboration between industry, researchers and government agencies through workshops and events run by its Joint Cyber Security Centres.

There has been a range of legislation enacted regarding the cyber security of Australia's critical infrastructure. The *Security of Critical Infrastructure Act 2018* (Cth), *Security Legislation Amendment (Critical Infrastructure) Act 2021* (Cth) and *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022* (Cth) apply to 11 sectors that are deemed to be critical infrastructure. Companies covered by this legislation need to meet additional cyber security obligations such as mandatory incident reporting to the ACSC, being subject to government intervention in response to a serious security incident if certain conditions are met and (for some entities) needing a risk management program (CISC 2022b).

Other legislation applies more broadly outside of critical infrastructure. Breaches of personal data are covered under the *Privacy Act 1988* (Cth) and breaches involving financial institutions are covered by the Prudential Standard CPS 234 on Information Security. There are also potential liabilities under the *Corporations Act 2001* (Cth) if 'directors failed to set up proper standards of cyber security to be implemented by management, for the protection of the company's business' (PwC 2017). For example, a financial advice company was recently found to have contravened the Corporations Act because of 'its failure to have documentation and controls in respect of cybersecurity and cyber resilience in place that were adequate to manage risk' (FCA 2022, p. i).

The Australian Government released a Ransomware Action Plan in October 2021, in part reflecting the significant growth in ransomware attacks reported to the ACSC (Home Affairs 2021b). It is intended to complement the broader initiatives and overarching approach outlined in the *Cyber Security Strategy*, with key elements introduced in the Crimes Legislation Amendment (Ransomware Action Plan) Bill 2022 in February 2022 (Parliament of Australia 2022). These included new criminal offences relating to ransomware attacks and stronger powers to investigate offshore cyber criminals and seize digital assets (Lim et al. 2022). The mandatory ransomware incident reporting scheme that was proposed in the Plan is still under development and was not included in this Bill. The Bill has since lapsed with the dissolution of Parliament in April 2022.

Providing information about good security practices and response

Government initiatives to improve cyber resilience and response should be 'light touch' where the risks are relatively low. This minimises the potential for unnecessary costs to be imposed on businesses while still supporting better security outcomes. Providing guidance to Australian businesses and individuals on how to build cyber resilience and respond appropriately to cyber attacks is one form of comparatively minimal intervention.

There is already a range of information published by the government about improving cyber security practices. The Australian Cyber Security Centre (ACSC) — which sits within the Australian Signals Directorate (ASD) — has various resources to assist individuals, small and medium businesses, larger organisations and critical infrastructure providers, and government agencies with mitigating, managing and anticipating cyber risks. These include:

- step-by-step guides that are more targeted towards individuals and smaller businesses, which outline basic and practical security instructions such as turning on automatic updates, using two-factor authentication and securing communication channels (ACSC 2020)
- material for larger and more mature organisations that require further guidance, including the 'Essential Eight' set of baseline mitigation strategies for cyber protection (ACSC 2021c) and the Information Security

> Manual, which advises organisations on selecting, implementing and assessing security controls in a way that is most relevant to their circumstances and risks (ACSC 2022b).

While widely available general guidance is useful, a previous study on small businesses' cyber security practices reported that there is:

> … a desire for targeted recommendations that speak to their specific circumstances. A key complaint about [the ACSC's website] is that the information is too general, which makes it hard for study participants to apply to their own circumstances. … Small businesses don't expect personalised support from free sources like [the ACSC's website], but the generic approach is not working. (Cynch Security et al. 2021, p. 31)

Improving the relevance and accessibility of general cyber security advice would require providing guidance based on businesses' specific operations and risk factors. Internationally, the Scottish Government has proposed the 'development of a freely accessible online tool to support SMEs, in particular, to undertake a cyber threat assessment… and be directed to appropriate guidance or standards' (Scottish Government 2018, p. 44). The Australian Government has a Cyber Security Assessment Tool, in which a business can complete an online survey about their industry, size, use of technology and current security practices (such as updating software, secure passwords, multi-factor authentication, information backups and incident planning) (DISER 2021). Based on their answers, businesses are assigned a cyber security maturity level using a four-point scale — from 'starter' to 'champion' — and provided with tailored suggestions, including actionable improvements and relevant links to the ACSC's step-by-step guidance.

However, SMEs continue to have relatively lower uptake of cyber security software, as discussed in section 2.2. More use of the interactive Cyber Security Assessment Tool by SMEs would support the adoption of more effective security practices and increase the value derived from information already published by the government. One channel for increasing awareness about this tool could be through industry associations — information could be shared between members, particularly to smaller businesses, about cyber security risks and tools for managing these risks.

Cyber security guidance can also help businesses and individuals to respond to incidents quickly and effectively after a breach occurs. Low and no-cost services are likely to have the highest uptake; for example, IDCARE is a not-for-profit organisation that provides free information and education to those who have been affected by cyber fraud. It is funded by subscribers such as major banks, government agencies and airlines, which themselves receive tailored incident response support (IDCARE 2022). The government has also published advice on cyber response, including in the ACCC's Scamwatch (ACCC 2022i) and the ACSC's ransomware response guide (ACSC 2021d). These initiatives collect and disseminate information from entities that have experienced cyber fraud, assisting other consumers and businesses to recover should they experience similar scams and ransomware incidents (ACCC 2021e, p. 72).

Regulation is required for high-risk situations

It is reasonable that situations posing greater cyber security risks to the broader Australian economy and society require stronger government activity than just providing guidance. Higher-risk cases include situations where a cyber attack on one entity could have widespread negative effects, such as where the entity has many interdependencies with and connections to other businesses and individuals (as discussed in section 2.2). It could also include instances where a cyber attack would reduce the availability of a service or asset that is essential to the functioning of the economy or society, such as water, energy or medical services.

More substantial government intervention could involve imposing regulation on companies for which an attack would represent a significant broader risk. Cyber security regulations must be designed and

implemented in a way that minimises unnecessary burdens, is not excessively intrusive and establishes clear expectations of the regulated entities. As summarised in box 3.5, the Australian Government has already passed several pieces of legislation regarding the cyber security of critical infrastructure sectors and assets, which have been identified as potentially facing higher risks. There are mixed views about the evolution of Australia's critical infrastructure legislation to date, regarding both the government's approach to developing and implementing the regulations, and its content.

On the approach, given the potential for these regulations to have large and complex impacts on businesses' core operations, industry consultation is important to enable government to understand the implications of its changes and address concerns about its approach, if possible. There has been some stakeholder engagement in developing the Australian legislation since the Department of Home Affairs first released its consultation paper in August 2020 (Home Affairs 2020b). However, industry stakeholders have observed that the *Security Legislation Amendment (Critical Infrastructure) Act 2021* (Cth) — which included broadening the definition of critical infrastructure, increased reporting obligations and new government intervention powers — was rushed following the recommendation of the Parliamentary Joint Committee on Intelligence and Security, which did not allow for suitable consultation (Karen 2021; Kwan 2021).

The Commission has heard from stakeholders that, while many affected companies appreciate the intent of critical infrastructure security legislation, inadequate consultation early in the process created significant uncertainty and apprehension. Companies observed that 'the "early days" of consultation had moved "a little too fast" and … it was more important to get things right than out the door' (Barbaschow 2021b). The Commission also heard that industry engagement has improved over time; for example, by incorporating small-group consultations rather than relying on large town-hall meetings, and clarifying and finessing definitions and rules. There are several instances where the Department of Home Affairs has revised the details of their approach following industry feedback, such as in relation to the risk management programs required by the *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022* (Cth) (Home Affairs 2022a).

Regarding the content of the legislation, specifying baseline cyber security obligations and reporting requirements for these higher-risk sectors is necessary government activity to protect national interests, given the negative externalities and information asymmetries involved (section 2.2). There may be opportunities to improve how these requirements are implemented; for example, more streamlined reporting to reduce overlapping obligations is discussed below. Broadly speaking, the Australian Government's actions are consistent with the increasing global regulatory activity in this space, as various other countries have also introduced cyber security regulations for critical infrastructure. These include the US's *Cyber Incident Reporting for Critical Infrastructure Act* (2022) and the EU's *Directive on Security of Network and Information Systems* (2016) (which has since been expanded to cover more critical sectors and entities).

The strongest element of Australia's critical infrastructure regulations is the government's new powers to intervene and assist a critical infrastructure provider in responding to a serious security incident. Industry feedback on this aspect of the legislation has been mixed: while some companies are open to receiving government assistance, as long as it is proportionate and done jointly with the company, others (especially in the technology sector) believe the harms of such government intervention outweigh the benefits (Barbaschow 2021a). In practice, the government may rarely have to use these powers if companies have suitable risk mitigation and management processes that minimise the likelihood of serious incidents occurring — and the rest of the critical infrastructure security obligations seek to ensure this is the case. However, the mere existence of intervention powers in the legislation could have the unintended consequence of deterring investment, particularly by multinational companies if Australia is ahead of other countries in implementing such requirements.

As it is early days, more time is required to assess whether the current suite of critical infrastructure regulations strike an appropriate balance between securing high-risk sectors while not unduly discouraging future growth. The government should monitor and evaluate the effectiveness and economic impact of implemented policies to improve its understanding of the trade off between security and growth, and recalibrate the regulations as required. Cyber security company Palo Alto Networks has observed that 'there is no independent review process articulated in the bill… this is contrary to some of the approaches taken in like-minded jurisdictions' (Williams 2022). An evaluation mechanism could also improve government's ability to incorporate industry feedback into its regulations.

Finding 4.16
Security regulations need to balance risk management and innovation impacts

Cyber security regulation of high-risk sectors needs to manage the risks without unnecessarily deterring businesses' innovation and investment. The impacts of the government's recent critical infrastructure security regulations remain unclear but, while more time and information is required to understand whether these regulations strike an appropriate balance, there is no evaluation or review process included in the legislation.

Streamlining incident reporting requirements to avoid duplication

There is currently no universal requirement for Australian businesses to report cyber security incidents. However, there are several mandatory reporting obligations for specific types of businesses that have experienced particular kinds of incidents (including under some of the Australian Government's cyber security initiatives summarised in box 3.5). These requirements relate primarily to operators of critical infrastructure, organisations that have experienced breaches of private personal data, financial organisations and proposals for large businesses that experience ransomware attacks.

- Under the *Security of Critical Infrastructure Act 2018* (Cth) (SOCI Act), and subsequent amendments, critical infrastructure asset owners and operators must report critical incidents (with a 'significant impact' on their asset) within 12 hours of becoming aware of the incident, and other security incidents (with a 'relevant impact' on their asset) within 72 hours. Reports must be made to the ACSC (CISC 2022a).
- The *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth) amended the *Privacy Act 1988* (Cth) to require organisations to 'notify affected individuals and the [Office of the Australian Information Commissioner] when a data breach is likely to result in serious harm to an individual whose personal information is involved' (OAIC nd). The scheme applies to all organisations covered by the Privacy Act, which includes Australian Government agencies and businesses with annual turnover of more than $3 million. The Privacy Act is currently being reviewed, and some submissions to the review have observed that 'small businesses [with turnover of less than $3 million] pose a significant cyber security risk… requiring small businesses to comply with the Act (in particular… the Notifiable Data Breaches Scheme) could be a mechanism to mitigate this risk' (AGD 2021, p. 42).
- In the financial services sector, the Prudential Standard CPS 234 on Information Security requires entities regulated by the Australian Prudential Regulation Authority (APRA) — including banks, insurers and superannuation funds — to notify the regulator of material information security incidents within 72 hours. Entities must also notify APRA of material information security control weaknesses within 10 business days (APRA 2019, p. 8).
- The current proposal for mandatory reporting in the Ransomware Action Plan requires businesses with annual turnover of more than $10 million to report ransomware attacks. Similar to the SOCI Act,

ransomware incidents with a 'significant impact' on a business would need to be made to the ACSC within 12 hours and incidents with a 'relevant impact' within 72 hours, with a follow-up report subsequently required to provide 'material details' about the incident (Lim et al. 2022).

Various other countries have similarly disparate requirements for cyber incident reporting. For example, in the United States, all 50 states have laws that require companies to notify residents if their sensitive personal data has been breached, but these requirements vary across states (such as needing to notify different parties or specifying different notice content and timing) (DLA Piper 2022). There are also federal laws, such as the recently passed the *Cyber Incident Reporting for Critical Infrastructure Act* (2022), which creates obligations to report cyber attacks on critical infrastructure. The numerous requirements can complicate compliance for businesses, particularly those operating in multiple states.

The proliferation of reporting requirements and the need to report to different agencies could place unnecessary burdens on businesses at an already challenging time, when they are focusing on recovering from the security breach. A more unified approach to reporting requirements would assist — the Australian Institute of Company Directors (sub. 44, p. 8) notes that 'the example of cyber incident reporting… reflects a tendency for governments and individual regulators to "go it alone" to respond to an emerging risk. … Without coordination across government, organisations and boards risk being swamped by complex, inconsistent and duplicative obligations'. The Australian Information Industry Association has also observed that disparate but overlapping cyber security reporting regimes place unnecessary red tape burdens on regulated companies (Smith 2022). The Insurance Council of Australia noted that overlapping cyber incident reporting requirements from the ACSC and APRA are 'compounding resource pressures for insurers, in a historically tight market' (ICA, sub. 203, p. 5).

Increasing coordination between government agencies can help to improve this situation, though coordination can also have its own costs, and these would need to be outweighed by the benefits of a more unified approach to incident reporting. For example, the UK Government has identified this as an area for improvement: one of the central pillars of its *Government Cyber Security Strategy: 2022 to 2030* is 'defend as one' (Cabinet Office 2022). This includes the creation of the Government Cyber Coordination Centre (GCCC), which aims to streamline the government's approach to cyber security, including incident reporting:

> [The UK] government will establish a cyber coordination centre to better coordinate operational cyber security efforts across government organisations and truly enhance government's ability to 'defend as one'… the GCCC will foster partnerships to rapidly identify, investigate and coordinate the response to incidents alongside threat and vulnerability reporting. (Cabinet Office 2022)

In addition, early and ongoing consultation with industry when designing and implementing various reporting obligations can help government to identify overlaps between separate requirements and, where possible, streamline these to avoid duplication. Coordination between policymakers and regulators, and the importance of industry engagement, are discussed more generally in section 3.6.

One option to simplify cyber security incident reporting would be to have a single interface or portal for Australian businesses to lodge all cyber incident-related reports required under various regulations. The operating system underlying the interface would then direct reports to the ACSC or relevant government agency as required to inform the response, without the business needing to make multiple reports or spend time identifying to whom and how they need to report. In the future, the government could work with software providers to build cyber incident reporting into commonly used cyber security software, so that reports are automatically sent to the relevant regulator if an incident occurs. This would be a similar approach to that taken by the ATO in working with software providers to build STP reporting into businesses' accounting software (section 3.2), although the coverage and functionality required in the cyber security reporting context is somewhat different.

Finding 4.17
Businesses experiencing security incidents can face multiple reporting obligations

A business may face multiple reporting requirements for a single cyber security incident, depending on its operations and the nature of the breach. This can place unnecessary burdens on businesses that are focused on recovering from the cyber incident. More coordination between government agencies and streamlining of reporting requirements (such as via a single online interface) would assist in reducing reporting burdens on businesses.

Recommendation 4.5
A single interface for cyber incident reporting

The cost for businesses of complying with cyber security regulations should be reduced by streamlining incident reporting requirements, with all reporting to occur via a single online interface. The operating system underlying this interface would then direct reports to the Australian Cyber Security Centre or other relevant government agency as required. This could provide the platform for the government to work with cyber security software providers to build incident reporting functions into commonly used software, so that reports are automatically sent to relevant agencies if an incident occurs.

Embedding cyber resilience and response into government

As users of digital and data tools themselves, governments also have their own responsibilities to build cyber resilience and adopt good security practices. There are a range of initiatives and guidance available to support government agencies in maintaining their cyber security obligations. These include:

- the Protective Security Policy Framework, which features policies on governance and information, personnel and physical security, and requires agencies to annually report their security maturity (AGD nd)
- the security criteria in the Digital Transformation Agency's Digital Service Standard for government services (DTA nd)
- the ACSC's Information Security Manual (discussed above)
- the whole-of-government *Hardening Government IT* initiative, which is being led by the Digital Transformation Agency and includes developing cyber hubs to centralise government agencies' capabilities in cyber threat monitoring, detection and response (DTA 2021).

In addition, the ASD provides direct assistance on cyber security to agencies. In 2020-21, this included conducting 14 cyber uplift activities with Commonwealth entities and publishing quarterly *Cyber Hygiene Improvement Programs* reports to government agencies (including undertaking 34 high priority operational tasking activities) (ASD 2021).

But in a world where increasing volumes of government transactions and services are digitised, more can be done to ensure that government's use of technology and the citizen data it holds are secure. This includes ensuring that all government employees, including those working outside IT functions, are sufficiently trained in basic security protocols to minimise the potential for human errors that could lead to cyber breaches. For example, between January and June 2021, the Office of the Australian Information Commissioner (OAIC) reported that 74% of the Australian Government's data breach notifications were due to human error — a significantly higher rate than the 30% observed across all sectors. The OAIC stated that 'human error

remains a major source of data breaches [and] the human factor also plays a role in many cyber security incidents… Organisations can reduce the risk of human error by educating staff about secure information handling practices and putting technological controls in place' (OAIC 2021).

Government agencies are also large consumers of technology: Gartner forecasts that in 2022, Australian governments — at the federal, state and territory and local levels — will spend almost $4.7 billion on software (up 19% on 2021 spend) and more than $6.4 billion on IT services (up 7%) (Govtech Review 2021). As purchasers of digital and data-related products, governments can encourage a greater focus on cyber resilience by incorporating security considerations into their procurement decisions. The Australian Strategic Policy Institute has made several suggestions on how this could be enacted:

> One suggested option has been to explicitly include security as a 'fourth pillar' in evaluating proposals, alongside cost, quality and timescales, although this then leaves subjectivity about how to measure security and weight it against the other criteria. A better approach would be an effective pricing mechanism, reflecting the fact that better security should equate to lower financial risk. (Shah 2020, p. 10)

This would incentivise potential suppliers to invest in good cyber security practices, without mandating requirements across all businesses. A similar measure is found in the US Government's *Executive Order on Improving the Nation's Cybersecurity* (The White House 2021). This stipulates that government agencies procuring in-scope software must 'receive attestation from the software producer that the software's development complies with government-specified secure software development practices' (NIST 2022, p. 3). These practices can include assurances that software producers maintain secure development environments (such as enacting multi-factor authentication, data encryption and relationship audits), maintain trusted source code supply chains or are regularly checking for vulnerabilities.

The ACSC provides guidance on how Australian organisations, including government agencies, can manage cyber supply chain risks (ACSC 2021b). Incorporating criteria about a software provider's security capabilities and cyber risk management practices explicitly into government procurement decisions would take this one step further, and incentivise organisations seeking to supply goods and services to improve their cyber resilience.

3.5 Supporting ethical use of technology and data

Emerging technologies such as AI, IoT and virtual and augmented reality have created ethical issues that may not relate directly to productivity, but can degrade trust in businesses' and governments' use of technology and data, which in turn limits adoption. In Australia, trust is the central driver for widespread acceptance of AI in particular: 'if people perceive AI systems to be trustworthy … this leads to the acceptance necessary to realise the potentially vast societal benefits that AI can produce' (Gillespie, Lockey and Curtis 2020, p. 48). This study also found that perceptions of the adequacy of AI regulations influence trust levels, and about two-thirds of surveyed Australians think that the government should regulate AI (with co-regulation between industry and government also widely supported) (Gillespie, Lockey and Curtis 2020, p. 24).

Ethical concerns about the use of technology and data have arisen around the world. Several well-publicised examples include:

- potential breaches of privacy associated with collecting and storing personal data, or using this data to influence human decisions, such as the Facebook–Cambridge Analytica case (Müller 2020)
- the ability of children to give informed consent for the collection and use of their data, particularly when service providers have complex privacy policies and use 'dark patterns' to nudge young people into accepting terms and conditions that they do not understand (Reset Australia 2021)

- unintended bias in automated decision making systems, such as an American criminal justice algorithm mislabelling African-American defendants as high risk at twice the rate of white defendants (Manyika, Silberg and Presten 2019)
- how to assign responsibility when using automated decision making systems, such as accidents involving autonomous vehicles that have been programmed to react to an oncoming crash by prioritising a driver over a pedestrian (Abu-Khalaf and Haskell-Dowland 2021; Awad et al. 2018).

A proactive approach to managing ethical issues is required to maintain trust while also avoiding hampering technological progress and innovation. There are a number of existing frameworks about the ethical use of technology and data, incorporating principles such as transparency, accuracy and privacy (box 3.6). The Consumer Policy Research Centre has stated that the government should take a holistic approach to data and digital policy 'guided by clearly articulated principles. Without it, the Government is at great risk of developing a policy environment which is not joined up or coherent… which will reduce productivity as well as undermine investment and community trust' (CPRC, sub. 19, p. 3).

Despite the prevalence of these frameworks, the challenge for businesses and governments is turning principles into action. Global examples of how businesses have implemented ethically responsible AI include having an ethics review board of subject matter and ethics experts, which provides advice or approval for ethics strategies and specific use cases (Eitel-Porter 2021), and adopting an 'ethics by design' policy to developing AI systems (EC 2021b).

Box 3.6 – Frameworks and principles guiding ethical use of technology and data

There are numerous frameworks in Australia and internationally that promote the ethical use of technology and data, mainly about the use of artificial intelligence (AI). These have been developed by governments and expert organisations; for example:

- the CSIRO's Data61 AI Ethics Framework discussion paper (Dawson et al. 2019) and the ensuing Department of Industry's Australia's Artificial Intelligence Framework (DISR 2019)
- the Australian Computer Society's AI Ethics Framework (ACS 2021c)
- the University of California's Responsible Artificial Intelligence report (UC 2021)
- the EU's proposed Artificial Intelligence Act (EIPA 2021)
- the US's *Algorithmic Accountability Act* (2019)
- the Office of the Privacy Commissioner of Canada's Regulatory Framework for AI (OPCC 2020)
- the UK's Data Ethics Framework (CDDO 2020)
- the New Zealand Privacy Commissioner and Government Chief Data Steward's principles for safe and effective use of data and analytics (OPCNZ and CDS 2018).

Many of these frameworks cover similar principles, suggesting that there is a strong consensus on how to manage and mitigate ethical risks in using AI and data analytics. Common elements include:

- transparency — informing individuals when AI-enabled tools are used and, to the extent possible, enabling them to understand the methods, potential outcomes, ways to challenge outcomes and remedies to address any harms caused
- accuracy, reliability and safety — developing AI-enabled tools that are effective, accurate and reliably operate in accordance with their intended purpose

Box 3.6 – Frameworks and principles guiding ethical use of technology and data

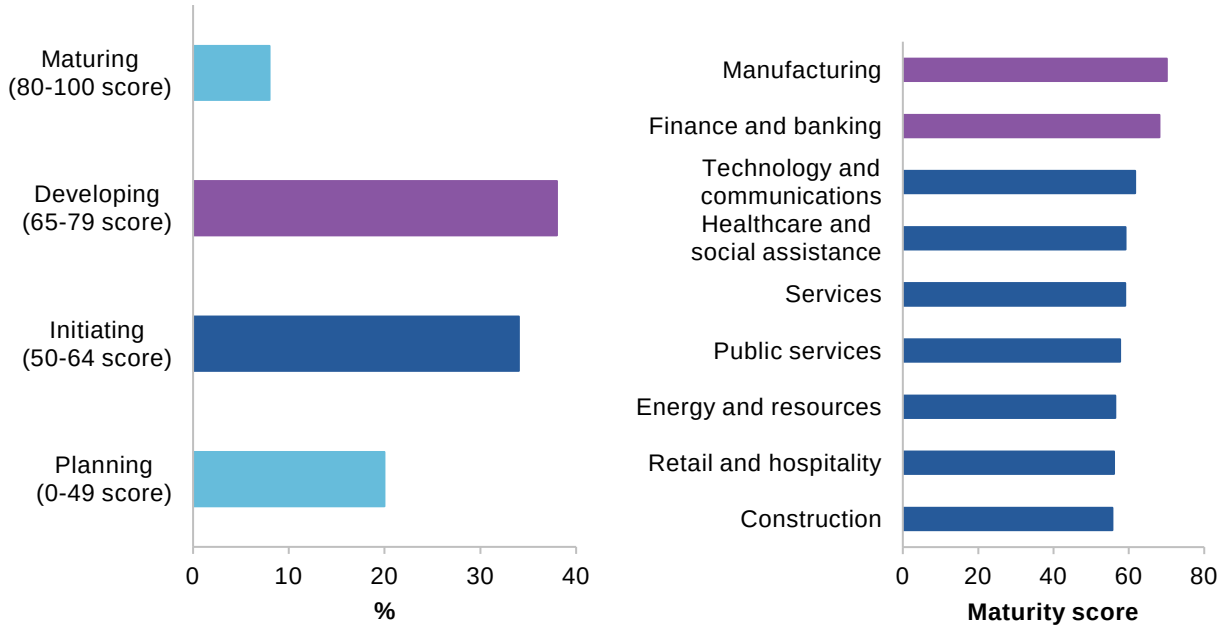
- fairness — assessing for bias and the risk that automated decisions unfairly discriminate against individuals, communities or groups. Procedures should be put in place to proactively identify, mitigate and remedy these harms
- privacy and security — designing AI-enabled tools to maximise the privacy and security of personal data
- human-centred values — developing and using AI-enabled tools in ways that respect human rights
- shared and net benefits — creating net benefits that are shared as broadly as possible, including across individuals, society and the environment
- accountability — holding developers and users of AI accountable for outcomes, including unintended consequences
- contestability and auditability — having an efficient and auditable process to allow people to challenge the use or output of an AI algorithm.

Most Australian companies are in the early stages of adopting ethically responsible technology practices, with the *Responsible AI Index 2021* finding that over 90% of surveyed companies were still planning, initiating or developing their AI ethics maturity (Fifth Quadrant, Ethical AI Advisory and Gradient Institute 2021, p. 10). There were industry-level differences in maturity levels, with manufacturing and finance leading the way (figure 3.14). The Committee for Economic Development of Australia reports a 'disconnect' in how organisations prioritise responsible use of and consumer trust in AI: 88% of participants in responsible AI workshops state that trust and consumer confidence in AI is a high priority for the future, but only 12% identify it as a current priority (CEDA 2022, p. 20).

On the government side, operationalising ethical principles is important for agencies to maintain their social licence to deliver digital and data-enabled government services, and for supporting confidence in public institutions more broadly. This is particularly crucial where technology is used to deliver sensitive or citizen-facing services. For instance, the 'Robodebt' automated debt assessment and recovery program — in which the government wrongly recovered payments from hundreds of thousands of Australians — illustrates how the inappropriate use of algorithmic decision making can more broadly damage trust in government (Rinta-Kahila et al. 2021; Tonkin 2021). The NSW Productivity Commission has pointed out that government policy should be cognisant of these issues as 'public aversion to technology can prevent its uptake ... and that could in turn stifle private innovation and productivity' (NSW PC 2022, p. 48).

Figure 3.14 – Most Australian companies are still developing their AI ethics maturity[a]

Distribution of responsible AI index maturity scores for all businesses and average scores by industry, 2021



a. The responsible AI index was created using data from a survey of 416 decision makers with influence over AI strategy at businesses with at least 20 employees.

Source: Fifth Quadrant et al. (2021, p. 11).

Government should adopt a risk-based approach

There are various policy options that can support the ethically responsible use of technology and data, ranging from information provision to regulation. Direct intervention and its potential benefits in improving confidence in emerging technology and data uses must be balanced against the potential costs incurred by businesses in complying with government requirements. A risk-based approach is appropriate to guide governments on where stronger activity is necessary, and provide clarity for businesses on where to focus their efforts on improving their ethics maturity.

Clearly defining different risk levels and identifying high-risk areas are key to designing government policy on technology and data ethics. Risk categories should be broad enough to cover the ethical use of different digital and data tools, by incorporating considerations around technology types, uses and the kinds of harms to be avoided. For example, unsupervised learning algorithms could fall into a higher risk category because 'there's a lack of transparency into how data is clustered' (Delua 2021), but if such an algorithm was used for relatively innocuous purposes, such as a chess game, it could fall into a lower risk category. Some guidance can be taken from risk-based approaches to ethical issues emerging overseas, such as the EU's regulatory framework on AI (figure 3.15) and the US's Algorithmic Accountability Act (2019), which defines a high-risk system as one that contributes to bias or makes decisions about 'sensitive aspects of consumers' lives' (United States' Congress 2019).

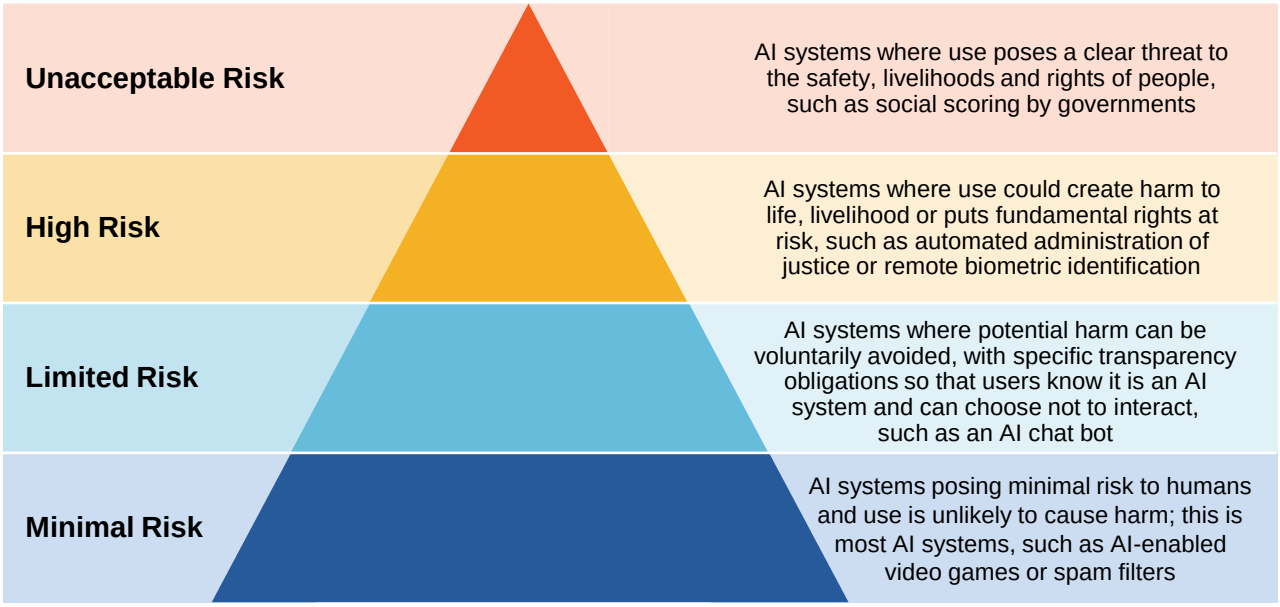
The extent to which high-risk areas need to be monitored by government and potentially require regulation is an open question for policymakers. Around the world, the European Union is currently the most active in exploring regulation for ethically responsible uses of technology and data, specifically for AI. The proposed

Artificial Intelligence Act prohibits AI that poses unacceptable risk (per figure 3.15) and introduces regulations for high-risk uses, such as the need to comply with data governance standards, have risk management systems in place and provide users with transparent information about their AI (EC 2021c, sec. 5,9,10,13). Even when taking a risk-based approach, it is challenging for governments to determine which regulations to apply in high-risk situations as they must balance the requisite protections with growth objectives; for example, the former Chief Executive Officer of Google has argued that the EU's AI transparency requirements are unviable and could stifle innovation (Haeck 2021).

It is vital that government consults widely with industry and technical experts when designing and implementing policy responses to high-risk ethical issues. This is partly because the technical details of emerging uses of technology and data can be challenging for policymakers to grasp, and stakeholder engagement promotes mutual understanding and reduces the possibility of introducing ineffective policies or unnecessarily restrictive regulations.

Figure 3.15 – The EU defines four levels of risk characterising AI systems

European Commission's regulatory framework proposal on AI



Source: EC (2022).

For example, in the case of AI regulation, the Australian Strategic Policy Institute observes that:

> …the current limitations in [understanding the 'black box' nature of decisions made by AI from large bodies of data] are the key problem in figuring out how to safely and ethically use and regulate AI… If we can't be certain of what correlations an AI is independently developing to inform data screening and decision-making, we can't be certain that either comply with safe and ethical principles. (Westendorf 2022, p. 5)

Ongoing consultation would also assist in identifying emerging areas that may be higher risk and require stronger intervention, as existing activities by both businesses and governments have predominantly focused on AI ethics. In the future, ethically responsible digital and data use will need to capture other types of technology and anticipate emerging issues. For example, there are likely to be ethical considerations arising from the collection of increasingly sensitive data and questions about how this data can be used — such as the growing ability to gather information about an individual's genetics, health and behaviours and whether it is appropriate for insurance

providers to access and use this data. Stakeholder engagement would help governments to improve their understanding of the potential harms of emerging uses of technology and data, determine whether these uses are genuinely high risk and consider the implications of any proposed policy responses.

The Australian Government has undertaken stakeholder consultations about automated decision making and AI regulation, covering issues such as public trust, transparency in outcomes and the potential for bias or discrimination (PMC 2022c, pp. 10–12). The Department of Industry, Science, Energy and Resources has also conducted an AI ethics principles pilot program with Australian businesses (including the Commonwealth Bank, Telstra, Insurance Australia Group and Flamingo AI) to better understand how ethical principles have been implemented in AI-related processes and products (DISER nd). This industry engagement has improved the government's understanding of new uses of technology and data and the ethical risks that can arise, while also creating valuable feedback loops between government and businesses about practical issues in applying ethical principles.

In addition to these initiatives that are specific to the ethical use of AI, the breadth of the common principles that guide technology and data-related ethics (box 3.6) means that various economy-wide policy frameworks may also apply to the use of AI and other digital tools. These include the cyber security regulations discussed in section 3.4, and privacy regulations for collecting and using data (box 3.7).

Box 3.7 – Privacy regulation needs to balance legal and economic concerns

Digital privacy regulation plays an important role in protecting individuals' rights, and unaddressed privacy issues 'can impact the community's trust and undermine the success of new technological and data initiatives by business and government' (OAIC, sub. 173, p. 3). Industry stakeholders acknowledge that the sheer scale of data held by businesses in the 21st century necessitates a comprehensive legislative approach to privacy protections and obligations (AIIA, sub. 180, p. 4). Clear privacy regulation is also important to guide technological innovation, such as the use of facial recognition software by retailers Bunnings, Kmart and The Good Guys, which was introduced without due consideration of the risks the technology could pose (CPRC, sub. 115, pp. 3–4).

Although there is a clear need for privacy safeguards, there are also trade-offs between more regulation and productivity and efficiency and, as such, the government should not focus solely on legal considerations in setting privacy regulation. For example, after the General Data Protection Regulation was introduced in the EU — placing strict privacy requirements on data sharing — rising compliance costs saw firm profits decrease by 8% and sales decrease by 2% (Presidente and Frey 2022). This primarily affected smaller businesses and there was 'no evidence that large technology companies, such as Facebook and Google, experienced any reductions in either sales or profits' (Presidente and Frey 2022). These effects of regulation on economic activity — especially potential distributional effects on smaller firms — need to be considered when creating digital privacy regulations. An overly legalistic focus on the need for privacy safeguards that is not coupled with a consideration of their costs in limiting data use, competition and technological innovation risks regulation swinging too far in the direction of restriction.

The costs of overly restrictive privacy regulations are not just felt by businesses, but also by individuals. Consumers value their privacy; however, they also place a high value on the products and services that are made available by data sharing. This contributes to a gap between people's stated expectations for online privacy and their online behaviour, or the 'privacy paradox' (Bongiovanni, Renaud and Aleisa 2020). For example, in 2017, 69% of Australians stated they were more concerned about online

Box 3.7 – Privacy regulation needs to balance legal and economic concerns

privacy than they were five years previously (OAIC 2017), but in the same year the Commission observed that 'more than 70 per cent of us hand over our personal data on social media. More than 80 cent of us are in a supermarket or airline loyalty program' (CEDA 2017). Individuals willingly hand over private data through Internet of Things devices (Aleisa, Renaud and Bongiovanni 2020), social networking and other technologies (Barth and De Jong 2017). Balancing consumer protection against consumer preferences is also important when designing privacy regulation.

The government should therefore ensure that when implementing privacy regulation — or when considering changes, such as in the current Privacy Act review — it consults widely with affected stakeholders to balance these legal and economic considerations, and targets interventions towards high-risk areas.

Finding 4.18
Translating principles of ethical use of technology into action is challenging

Governments have generally agreed on the principles of ethical use of artificial intelligence, but are still working out how to translate this into action and where policy intervention is required. Given the trade-offs between regulation (including existing economy-wide regulations, such as around privacy) and potential productivity gains, any intervention would need to be appropriately targeted towards high-risk areas, and implemented in consultation with industry and technical experts.

3.6 Coordinating the policy and regulatory environment

The diversity, complexity and pace of change of technology use can make it challenging for governments to design and implement appropriate policy and regulatory frameworks. In addition, while the ever-increasing amounts of data produced in the Australian economy and society provides new opportunities to create value, it also gives rise to new considerations. Some of the issues that governments must grapple with in setting digital and data policy and regulation include:

- ensuring that policy frameworks are fit for purpose — policy settings must be appropriately calibrated throughout the policy life cycle. Given the potential for rapid technological change, they need to respond quickly to issues arising from new digital and data uses so that they remain fit for purpose, such as by taking an adaptive approach to regulation (Eggers, Turley and Kishnani 2018). This also helps to avoid regulatory overreach, as settings can be adjusted if they are unnecessarily restrictive
- enforcing regulation when boundaries are blurred — many uses of technology and data challenge traditional market definitions, including by blurring the definition between consumers and producers, or digital and data service transactions taking place across national boundaries. This can make it difficult to attribute responsibility and enforce laws (OECD 2020, chap. 1)
- accommodating interactions and broader business model changes — the benefits and risks associated with a specific technology can be magnified when it is used in conjunction with other technologies, or when applied to large volumes of data. They can also derive from changes to broader decision making processes or even entire business models (see, for example, CompTIA 2020), and these must be accounted for in designing policy and regulation

- avoiding technological protectionist policies — businesses that stand to lose from new uses of digital and data could seek government assistance and protection through regulation, subsidies or policies that increase the costs of technologically advanced rivals (Lambert 2021). Governments should be wary of vested interests, as these types of intervention would likely slow technology adoption and stymie new innovations.

Given these considerations, focusing policy settings too narrowly on an individual technology or a single aspect of data use is likely to be ineffective. Such an approach risks creating disparate regulations that target specific problems, and this kind of piecemeal regulatory environment could lead to additional uncertainty or costs for businesses, deterring adoption of productivity-enhancing uses of technology and data. For example, various cyber security regulations that seek to address different security risks and sectors have led to multiple incident reporting requirements for some businesses, as discussed in section 3.4. The Tech Council of Australia submitted that government should take 'a holistic approach to regulation… [and] provide regulators with clear expectations and accountability for considering the need to minimise uncertainty and compliance costs' (TCA, sub. 51, pp. 18–19).

Australia has also, at times, taken a reactionary approach to addressing specific digital, data and cyber security issues. This may have unintended consequences, whereby legislation intended to address a narrow issue or sector eventually has a broader impact, due to the interlinked nature of digital and data activities. For instance, the *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019* (Cth), criminalising violent online content in response to the 2019 Christchurch terrorist attacks, and *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth), allowing government to access encrypted communications, were both 'drafted very broadly and much of the criticism has focussed on the unintended consequences that arise from that approach' (Chatwood and Allen 2019). But the urgency with which these laws were designed and passed, in order to respond to particular concerns, meant that consultation about their potential broader implications was limited.

Many of the policy areas where there has been piecemeal or reactive activity are issues that are worthy of government attention. However, government responses would be more effective at supporting emerging digital and data uses if they were better coordinated, with industry previously observing that a regulatory framework that is 'largely piecemeal and lacks coordination, potentially creat[es] suboptimal implementations of many [regulatory] initiatives' (Data Republic 2020, p. 15). In interviews with government, regulators, industry and civil society about effective approaches to technology regulation, the Tech Policy Design Centre found that a common theme was 'calls for consistent political leadership and improved coordination between and among regulators and policy agencies' (Weaver and O'Connor 2022, p. 8).

More coordination between different government agencies with oversight over digital, data and cyber security issues would likely improve decision making and reduce uncertainty for regulated entities. Such coordination also provides a forum for agencies to discuss good practices and successful approaches to designing and implementing policy and regulation, including how they have navigated the complexities described above. For example, agencies could share information about emerging risks or unintended consequences of particular regulations. They could also work together to identify areas of duplication or inconsistencies in their respective activities — coordination on these matters is particularly important in areas where government sets minimum standards or supports technology or data interoperability between different parts of the economy.

Recognising the benefits of increased coordination, the UK Government formed the Digital Regulation Cooperation Forum (DRCF) in 2020. It now comprises the Competition and Markets Authority (which regulates competition in digital markets), Information Commissioner's Office (personal data protection), Office of Communications (online safety and communications security) and Financial Conduct Authority (online financial scams). The DRCF enables joint responses to technological developments that cut across multiple areas, more coherent regulatory approaches for interrelated issues (for example, overlaps between

data protection and competition regulation) and collectively developing technical expertise and analytical capabilities (CMA 2021). In 2021 to 2022, it created cross-regulatory teams across participating agencies covering four digital and data topics: algorithmic processing, regulatory design frameworks, digital advertising technologies and end-to-end encryption (DRCF 2022).

More recently in Australia, the Digital Platform Regulators Forum (DP-REG) was established in March 2022 to improve coordination on digital platform regulation between the ACCC, ACMA, OAIC and Office of the eSafety Commissioner. DP-REG will meet every two months to 'share information about, and collaborate on, cross-cutting issues and activities relating to the regulation of digital platforms [such as] how competition, consumer protection, privacy, online safety and data intersect' (DP-REG 2022, p. 1). At its first meeting, DP-REG members identified transparency and accountability of digital platforms' activities, the impact of algorithms such as in product recommendations and harmful content, and collaboration and capacity building between the four regulators as priorities for 2022/23 (ACCC 2022c). The regulators involved have benefited from using the forum to improve their assessment of emerging digital risks and deepen their engagement with relevant stakeholders (eSafety Commissioner, sub. 87, p, 4; OAIC, sub. 173, p. 11).

Stakeholders have observed that improving coordination between government agencies that design and implement policy and regulation would be beneficial more broadly across digital and data issues (not just for digital platforms), and that it could provide a forum for more industry engagement. For example, the Australian Information Industry Association suggested that:

> … the relevant people who are creating laws and policies that govern the tech sector should come together and work on any new regulation and industry needs to be part of that process. It would stop this fairly siloed, knee-jerk response to issues as they arise ... If you get better policy outcomes and industry endorse it, then it's good for government. (Smith 2022)

The Tech Policy Design Centre notes that both the DRCF and DP-REG comprise regulators only, and proposes a coordination model that includes both regulators and policymakers. Its preferred Tech Policy and Regulator Coordination Model 'takes an ecosystem wide approach [that] responds to calls for political leadership, strengthened coordination, increased transparency, access to independent technical expertise, and regularised, meaningful input by industry and civil society [but] does not alter the independent mandates of existing policy owners or regulators' (Weaver and O'Connor 2022, p. 10). While the DRCF and DP-REG do not have a formal mechanism for other stakeholders to participate, the proposed Tech Policy and Regulator Coordination Model includes both an Expert Forum to seek regular input from industry and civil society, and an Advisory Panel that would provide ad-hoc technical expertise as required (Weaver and O'Connor 2022, pp. 12, 14).

In addition, more coordination between domestic policymakers and regulators provides a platform for Australia to better engage with policymakers and regulators in other countries on technology and data issues, which often spill across international borders in a digital world. This is important for collaborating on global policy areas such as cross-border data flows, with the World Economic Forum highlighting that:

> …progressive cross-border data flows policy has come into its own as a policy lever for ambitious governments seeking economic recovery. [However,] laws and policies that act as barriers to this type of international data sharing are on the rise… slowing technological innovation and limiting positive societal impact. (WEF 2020a, p. 5)

There can be cross-country differences in digital and data regulations and policy frameworks. While this often justifiably reflects different countries' priorities and constituents, it can create additional burdens for businesses that operate in multiple jurisdictions. They may face extra costs in meeting inconsistent requirements, and potentially withdraw from smaller markets where regulations differ from those in larger markets because the costs outweigh the benefits of conforming to an additional set of rules. Greater international engagement between policymakers

and regulators would support the development of 'interoperable policy frameworks that can streamline requirements across borders and create mechanisms to reduce regulatory overload' (WEF 2020a, p. 5).

Where cross-country inconsistencies in digital and data policies and regulations persist, international engagement would help Australian government agencies to understand the varying requirements of other jurisdictions. If other countries have adopted requirements on matters such as data security or consumer protections that differ to Australia's but partly or fully address local concerns, domestic authorities could take approvals from these other countries into account when assessing whether a business has met Australian requirements. This approach is already used in some other sectors requiring regulatory approval — for example, in medicinal manufacturing, Australia's Therapeutic Goods Administration has agreements with other countries' authorities that allow it 'to use inspections conducted by these regulatory authorities as part of the [Good Manufacturing Practice] clearance process in lieu of performing our own on-site inspection' (TGA 2017). And in food safety, Australia has a recognition agreement with the US Food and Drug Administration, 'recognising Australia's food safety system and the US food safety system are comparable/ equivalent to each other' (DAWE 2022).

Finally, increased coordination between government agencies — and more engagement with industry and overseas regulators and policymakers — can have financial and time costs. Some formal coordination mechanisms need dedicated resources (such as a secretariat), and even models that simply involve regular meetings between agencies will require existing staff to make time to prepare for and attend these meetings. These costs should be weighed against the economy-wide benefits of improving coordination in determining the appropriate model to be implemented.

Finding 4.19
Greater coordination in digital and data policy could support technology adoption

Existing coordination between Australian government agencies on technology and data issues only includes regulators, not policymakers, and focuses on digital platforms. More coordination could reduce uncertainty for regulated entities and improve engagement with industry and overseas, supporting adoption of productivity-enhancing technologies. The benefits of this would need to be weighed against the potential financial and time costs of greater coordination.

Appendices

A. Modelling business technology adoption

This appendix provides additional details on the logistic regressions discussed in chapter 1. The regressions use 2019-20 Business Characteristics Survey data, which was accessed from the Business Longitudinal Analysis Data Environment.

A logistic regression was estimated for each type of technology that businesses were asked if they used.[18] Technology use was the dependent variable for each regression, with this variable taking the value of 0 if the business did not use the technology and 1 if the business used it. The independent variables were a series of dummy variables indicating the industry, region and number of employees of the business. Baseline categories were the primary industries industry, major cities of Australia region and 0 to 4 employees.

$$
\begin{aligned}
&Technology\ Type \\
&\quad = \beta_0 + \beta_1 Manufacturing + \beta_2 Electricity, Water\ and\ Waste\ Services + \beta_3 Construction \\
&\quad + \beta_4 Supply\ Chain\ Logistics + \beta_5 Customer\ Services \\
&\quad + \beta_6 Information\ Media\ and\ Telecommunications + \beta_7 Knowledge\ Services \\
&\quad + \beta_8 Other\ Services + \beta_9 Inner\ Regional\ Australia \\
&\quad + \beta_{10} Outer\ Regional\ and\ Remote\ and\ Very\ Remote\ Australia + \beta_{11} 5\ to\ 19\ Employees \\
&\quad + \beta_{12} 20\ to\ 199\ Employees + \beta_{13} 200\ or\ more\ Employees
\end{aligned}
$$

Table A.1 – Relationship between business characteristics and technology use (1)
Logistic regression results using 2019-20 Business Characteristics Survey data[a]

	Customer Relationship Management software	Enterprise Resource Planning software	Electronic Data Interchange	Radio Frequency Identification tags
Intercept	-2.62 ***	-2.47 ***	-2.62 ***	-3.35 ***
	(0.16)	(0.2)	(0.16)	(0.24)
Ind_Manufacturing	0.84 ***	-0.25	0.55 **	-0.57 *
	(0.19)	(0.22)	(0.19)	(0.24)
Ind_Electricity_Water_and_Waste_Services	0.92 ***	-0.47	0.5 *	-0.38
	(0.23)	(0.29)	(0.23)	(0.32)

[18] The technology types asked about in the 2019-20 Business Characteristics Survey were customer relationship management software, enterprise resource planning software, electronic data interchange, radio frequency identification devices, cloud technology, cybersecurity software, data analytics, internet of things, artificial intelligence, 3D printing, blockchain technology and allowed respondents to indicate if they used other types of technologies or none of the above.

	Customer Relationship Management software	Enterprise Resource Planning software	Electronic Data Interchange	Radio Frequency Identification tags
Ind_Construction	0.31	-1.14 ***	0.15	-1.23 ***
	(0.21)	(0.25)	(0.21)	(0.32)
Ind_Supply_Chain_Logistics	0.83 ***	-0.46 *	0.81 ***	-0.46 *
	(0.18)	(0.21)	(0.17)	(0.22)
Ind_Customer_Services	0.57 **	-1.61 ***	0.46 **	-1.12 ***
	(0.17)	(0.2)	(0.17)	(0.23)
Ind_Information_Media_and_Telecommunications	1.63 ***	-0.25	0.45 *	-0.64
	(0.21)	(0.26)	(0.22)	(0.34)
Ind_Knowledge_Services	1.75 ***	-0.91 ***	0.45 **	-0.9 ***
	(0.17)	(0.2)	(0.17)	(0.23)
Ind_Other_Services	1.26 ***	-1.49 ***	-0.01	-1.17 ***
	(0.17)	(0.19)	(0.16)	(0.21)
Reg_inner_regional_australia	-0.31 **	-1.33 ***	-0.07	-0.34
	(0.1)	(0.18)	(0.11)	(0.21)
Reg_outer_regional_and_remote_and_very_remote_australia	-0.66 ***	-1.16 ***	-0.27	-0.24
	(0.15)	(0.22)	(0.15)	(0.25)
Employee_Size_5_to_19_employees	0.77 ***	0.92 ***	0.87 ***	0.84 ***
	(0.09)	(0.17)	(0.1)	(0.23)
Employee_Size_20_to_199_employees	1.36 ***	2.51 ***	1.42 ***	1.65 ***
	(0.1)	(0.15)	(0.11)	(0.23)
Employee_Size_200_or_more_employees	2.2 ***	4.31 ***	2.44 ***	3.28 ***
	(0.09)	(0.15)	(0.1)	(0.19)
N	5469	5469	5469	5469
McFadden's pseudo R-squared	0.16	0.39	0.15	0.22

a. ***, **, * respectively indicate statistically significant coefficient estimates at the 0.1, 1, 5% levels.

Source: Productivity Commission estimates using data in the ABS's Business Longitudinal Analysis Data Environment.

Table A.2 – Relationship between business characteristics and technology use (2)

Logistic regression results using 2019-20 Business Characteristics Survey data[a]

	Cloud technology	Cybersecurity software	Data analytics	Internet of things
Intercept	-0.59 ***	-1.22 ***	-2.57 ***	-2.32 ***
	(0.11)	(0.12)	(0.18)	(0.17)
Ind_Manufacturing	-0.2	-0.1	-0.49 *	-0.12
	(0.15)	(0.16)	(0.21)	(0.2)
Ind_Electricity_Water_and_Waste_Services	0.06	0	0.14	0.41
	(0.18)	(0.2)	(0.26)	(0.23)
Ind_Construction	-0.24	-0.51 **	-1.15 ***	-0.43
	(0.15)	(0.17)	(0.27)	(0.23)
Ind_Supply_Chain_Logistics	-0.21	-0.14	-0.36	-0.62 **
	(0.13)	(0.14)	(0.2)	(0.2)
Ind_Customer_Services	-0.41 **	-0.56 ***	-0.75 ***	-0.79 ***
	(0.12)	(0.13)	(0.19)	(0.18)
Ind_Information_Media_and_Telecommunications	0.69 ***	0.21	0.9 ***	0.32
	(0.17)	(0.18)	(0.23)	(0.22)
Ind_Knowledge_Services	0.73 ***	0.62 ***	0.28	-0.2
	(0.12)	(0.13)	(0.18)	(0.17)
Ind_Other_Services	0.09	0	-0.63 ***	-0.56 **
	(0.12)	(0.13)	(0.18)	(0.17)
Reg_inner_regional_australia	-0.14	0.04	-0.58 ***	-0.15
	(0.08)	(0.09)	(0.15)	(0.14)
Reg_outer_regional_and_remote_and_very_remote_australia	-0.16	-0.03	-0.36	-0.4 *
	(0.11)	(0.12)	(0.19)	(0.19)
Employee_Size_5_to_19_employees	0.75 ***	0.58 ***	0.42 **	0.58 ***
	(0.07)	(0.08)	(0.14)	(0.13)
Employee_Size_20_to_199_employees	1.2 ***	1.32 ***	1.47 ***	1.01 ***
	(0.09)	(0.09)	(0.14)	(0.14)
Employee_Size_200_or_more_employees	1.73 ***	2.37 ***	3.13 ***	1.92 ***
	(0.08)	(0.09)	(0.12)	(0.11)
N	5469	5469	5469	5469
McFadden's pseudo R-squared	0.09	0.14	0.25	0.10

a. ***, **, * respectively indicate statistically significant coefficient estimates at the 0.1, 1, 5% levels.

Source: Productivity Commission estimates using data in the ABS's Business Longitudinal Analysis Data Environment.

Table A.3 – Relationship between business characteristics and technology use (3)

Logistic regression results using 2019-20 Business Characteristics Survey data[a]

	Artificial intelligence	3D Printing	Blockchain technology
Intercept	-3.99 ***	-4.91 ***	-5.9 ***
	(0.29)	(0.45)	(0.76)
Ind_Manufacturing	-0.17	1.28 **	0.45
	(0.32)	(0.44)	(0.88)
Ind_Electricity_Water_and_Waste_Services	0.56	0.78	1.37
	(0.37)	(0.55)	(0.88)
Ind_Construction	-1.08 *	0.36	0.15
	(0.46)	(0.53)	(1.01)
Ind_Supply_Chain_Logistics	-0.16	-0.13	0.53
	(0.3)	(0.5)	(0.83)
Ind_Customer_Services	-1.1 ***	-0.7	0.13
	(0.33)	(0.52)	(0.83)
Ind_Information_Media_and_Telecommunications	1.05 **	0.34	2.08 **
	(0.34)	(0.61)	(0.8)
Ind_Knowledge_Services	0.94 ***	0.51	1.8 *
	(0.27)	(0.44)	(0.74)
Ind_Other_Services	-0.46	-0.62	0.02
	(0.28)	(0.47)	(0.8)
Reg_inner_regional_australia	-0.79 **	-0.52	0.01
	(0.27)	(0.38)	(0.39)
Reg_outer_regional_and_remote_and_very_remote_australia	-0.58	0.1	-0.58
	(0.34)	(0.39)	(0.74)
Employee_Size_5_to_19_employees	0.59 **	0.81 **	0.77 *
	(0.22)	(0.31)	(0.34)
Employee_Size_20_to_199_employees	1.04 ***	0.93 **	0.64
	(0.24)	(0.35)	(0.44)
Employee_Size_200_or_more_employees	2.83 ***	1.93 ***	1.46 ***
	(0.18)	(0.27)	(0.32)
N	5469	5469	5469
McFadden's pseudo R-squared	0.21	0.10	0.08

a. ***, **, * respectively indicate statistically significant coefficient estimates at the 0.1, 1, 5% levels.

Source: Productivity Commission estimates using data in the ABS's Business Longitudinal Analysis Data Environment.

B. Stylised simulations of economy-wide effects

Regional and remote digital infrastructure[19]

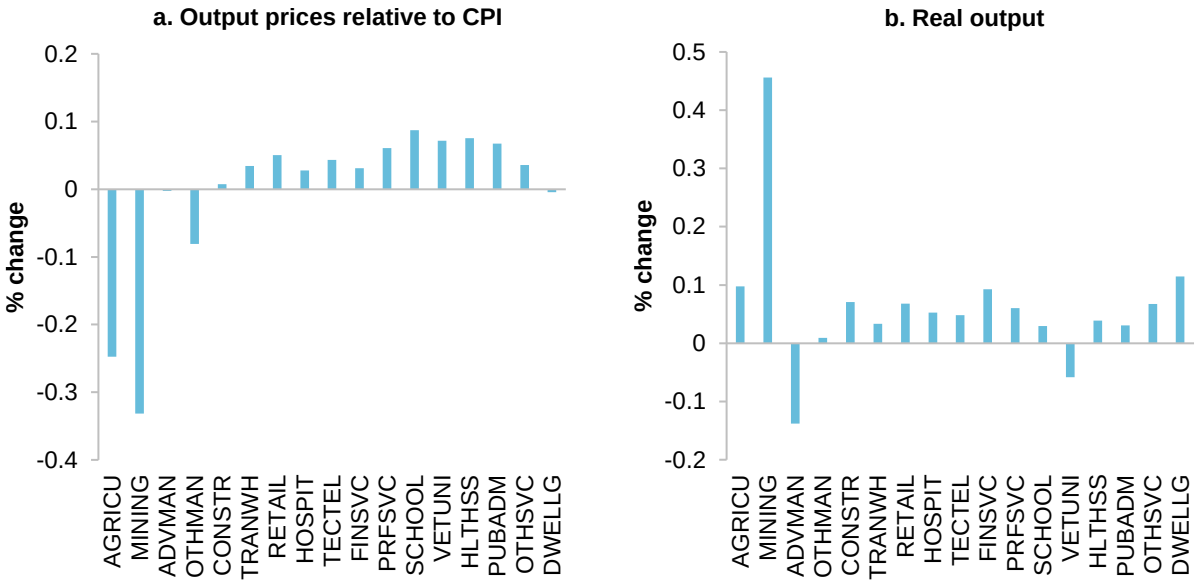
The Commission used a whole-of-economy model to simulate the increased use of technology and data in regional and remote areas that could result from improved digital infrastructure. This model is static, in that it does not capture dynamic effects over time. Rather, the results are interpreted as if the effects of a shock to the economy could happen overnight. While the simulation is stylised and there is a high level of uncertainty in the impacts of the proposed recommendation and other model assumptions, the simulation provides insight on how potential productivity improvements could flow through the economy's structure and the differential impacts across industries and household types. Further details of the model, simulation and effects of sensitivity testing are contained in this inquiry's companion volume *Whole-of-economy modelling*.

In this simulation, the efficiency with which the 'mining' and 'agriculture, forestry and fishing' industries use labour and capital was increased such that they could produce 0.5% more output using the same quantity of labour and capital. While other industries operating in regional and remote areas are likely to benefit from improved digital infrastructure as well, shocks to 'mining' and 'agriculture, forestry and fishing' industries were simulated due to their much higher shares of labour (as a proxy for output) in regional and remote areas.

The increased productivity in the 'mining' and 'agriculture, forestry and fishing' industries resulted in a reduction in prices relative to the economy-wide consumer price index (CPI) of commodities produced by these industries (figure B.1, panel a) which, in turn, increased demand for their outputs. The increased demand came from both domestic and foreign consumption: on the latter, lower relative prices of commodities produced by the 'mining' and 'agriculture, forestry and fishing' industries meant that they were relatively cheaper in the foreign market, leading to an increase in the quantity of these commodities exported.

[19] Referred to as simulation 2 in this inquiry's companion volume *Whole-of-economy modelling*.

Figure B.1 – Estimated change in output prices and real output by industry[a]



a. Industry abbreviations: AGRICU – agriculture, forestry and fishing; MINING – mining; ADVMAN – advanced manufacturing; OTHMAN – other manufacturing; CONSTR – construction; TRANWH – transport and wholesale; RETAIL – retail trade; HOSPIT – hospitality; TECTEL – technology and telecommunications; FINSVC – financial services; PRFSVC – professional, scientific and technical services; SCHOOL – school education; VETUNI – technical, vocational and tertiary education; HLTHSS – health and social services; PUBADM – public administration; OTHSVC – other services; DWELLG – ownership of dwellings.

Source: Productivity Commission estimates.

The quantity of output produced grew across most industries, not only in the shocked industries (figure B.1, panel b), due to aggregate demand effects, for example through household consumption increasing due to higher incomes. However, this was not the case for the 'advanced manufacturing' and 'technical, vocational and tertiary education' industries due to their relatively higher export intensity and the model's assumptions about fixed foreign investment.[20] Across the entire economy, real GDP and real gross national income increased by about 0.1% in this simulation. The magnitude of results depended on model and simulation assumptions; for example, sensitivity testing found that the real GDP effect ranged from about 0.04 to 0.20% with different assumed shock sizes, demonstrating the uncertainty in the simulations (chapter 4 of this inquiry's companion volume *Whole-of-economy modelling*).

Labour used by the 'mining' and 'agriculture, forestry and fishing' industries decreased because they required less labour to produce the same amount of output. The increased demand for these commodities was not large enough to induce an overall increase in demand for labour in those industries. Across the economy, there was an overall increase in labour use and real wage rates (that is, wages relative to the economy-wide CPI) due to

[20] Exports were a relatively large share of demand for these industries' outputs (making up about a quarter of the value of output before the simulated productivity increase). Assumptions in the model about fixed foreign investment mean that movements in the balance of trade are limited; therefore the increased exports of 'mining' and 'agriculture, forestry and fishing' commodities came with a fall in exports of other goods and services. For the 'advanced manufacturing' and 'technical, vocational and tertiary education' industries, these falls were greater than increases in domestic demand.

increased demand for other commodities. The increase in real wage rates contributed to the relative price increases for most industries that were not affected by the productivity shock.[21]

There was also an overall economy-wide increase in the capital stock. 'Mining' and 'agriculture, forestry and fishing' industries were relatively capital-intensive, so the productivity improvements in these industries led to proportionally large decreases in the need for capital in the economy to produce the same amount of output. However, this was mitigated by increased demand for capital arising from increased demand for goods and services across the economy, along with a lower relative price of investment and capital rental.

Households increased their real consumption of all commodities. The increase in real wage rates and overall labour use resulted in real labour income increasing across all age groups, genders and education levels, while the increased amount of capital held by households led to an increase in real capital income, despite relative falls in the capital rental price. These increases in income (which more than offset increases in saving and income taxes) meant that households increased their consumption of all other commodities, even with the majority of these commodities seeing relative price increases. Household wellbeing increased as a result of higher consumption, with the value of the increase estimated to be about $1.1 billion in 2018-19 dollars (that is, if this amount was given as extra income instead of the productivity shock, households would be as well off as they were estimated to be after the productivity shock).

[21] Relative prices of outputs produced by the 'other manufacturing' industry decreased (figure B.1, panel a). This industry relies relatively heavily on 'mining' and 'agriculture, forestry and fishing' outputs as intermediate inputs (which constituted about 25% of production costs before the simulation), so the falls in prices of these outputs flowed through to the price of 'other manufacturing' outputs.

Abbreviations

ABS	Australian Bureau of Statistics
ACCC	Australian Competition and Consumer Commission
ACMA	Australian Communications and Media Authority
ACSC	Australian Cyber Security Centre
AI	Artificial Intelligence
ANZSCO	Australian and New Zealand Standard Classification of Occupations
ANZSIC	Australian and New Zealand Standard Industrial Classification
APRA	Australian Prudential Regulation Authority
ASD	Australian Signals Directorate
ATO	Australian Taxation Office
BLADE	Business Longitudinal Analysis Data Environment
CDR	Consumer Data Right
COVID-19	Coronavirus disease (an infectious disease caused by the SARS-CoV-2 virus)
CRM	Customer relationship management
CSIRO	Commonwealth Scientific and Industrial Research Organisation
DAT	Data Availability and Transparency
DP-REG	Digital Platform Regulators Forum
DRCF	Digital Regulation Cooperation Forum
EDI	Electronic data interchange
ERP	Enterprise resource planning
EU	European Union
GCCC	Government Cyber Coordination Centre
GDP	Gross Domestic Product
GP	General Practitioner
IT	Information Technology
IoT	Internet of Things
ICT	Information and Communication Technology
MADIP	Multi-Agency Data Integration Project
Mbps	Megabits per second
MBSP	Mobile Black Spot Program
MHR	My Health Record

NBN	National Broadband Network
NDIA	National Disability Insurance Agency
NDIS	National Disability Insurance Scheme
NSC	National Skills Commission
OAIC	Office of the Australian Information Commissioner
OECD	Organisation for Economic Co-operation and Development
PC	Productivity Commission
PHN	Primary health network
PIP QI	Practice Incentives Program Quality Improvement
RCP	Regional Connectivity Program
RFID	Radio-frequency identification
SaaS	Software-as-a-Service
SME	Small and medium enterprise
SOCI	Security of Critical Infrastructure
STP	Single Touch Payroll
TSS	Temporary Skill Shortage
UK	United Kingdom
UN	United Nations
US	United States
USG	Universal Service Guarantee
USO	Universal Service Obligation
VET	Vocational Education and Training

References

ABS (Australian Bureau of Statistics) 2018, *Summary of IT Use and Innovation in Australian Business 2016-17*, Cat. no. 8166.0.

—— 2021a, *Characteristics of Australian Business, 2019-20*, Cta. No. 8167.0.

—— 2021b, *Characteristics of Australian Business methodology*, released 4 June.

—— 2022a, *BLADE Research Projects*, https://www.abs.gov.au/about/data-services/data-integration/integrated-data/business-longitudinal-analysis-data-environment-blade/blade-research-projects (accessed 17 May 2022).

—— 2022b, *Digital activity in the Australian economy, 2020-21*, https://www.abs.gov.au/articles/digital-activity-australian-economy-2020-21 (accessed 7 December 2022).

—— 2022c, *Multi-Agency Data Integration Project (MADIP) Research Projects*, https://www.abs.gov.au/about/data-services/data-integration/integrated-data/multi-agency-data-integration-project-madip/multi-agency-data-integration-project-madip-research-projects (accessed 17 May 2022).

—— nd, *Deregulation at the ABS*, https://www.abs.gov.au/about/key-priorities/deregulation-abs (accessed 16 May 2022).

Abu-Khalaf, J. and Haskell-Dowland, P. 2021, 'The self-driving trolley problem: how will future AI systems make the most ethical choices for all of us?', *The Conversation*.

Academy Xi 2022, *Online courses*, https://academyxi.com/online-courses/ (accessed 17 May 2022).

ACCC (Australian Competition and Consumer Commission) 2007, *Submission to the DCITA review of the universal service obligation (USO)*, November.

—— 2016, *ACCC submission to the Productivity Commission's Issues Paper on the Telecommunications Universal Service Obligation*, July.

—— 2020, *Report on modelling of the Regional Broadband Scheme levy initial base component*, October.

—— 2021a, *Internet Activity Report: For the period ending 30 June 2021*, December.

—— 2021b, *Mobile Infrastructure Report 2021*, December.

—— 2021c, *Mobile network investment continues but focus is on 5G in major cities*, https://www.accc.gov.au/media-release/mobile-network-investment-continues-but-focus-is-on-5g-in-major-cities (accessed 13 May 2022).

—— 2021d, *Superfast Broadband Access Service and Local Bitstream Access Service declaration inquiry: Final Decision*.

—— 2021e, *Targeting scams: Report of the ACCC on scams activity 2020*, June.

—— 2022a, *ACCC launches CDR Sandbox to assist participant design, build & testing*, https://www.accc.gov.au/media-release/accc-launches-cdr-sandbox-to-assist-participant-design-build-testing (accessed 25 July 2022).

—— 2022b, *ACCC'S Post: Waave Technologies joins the Consumer Data Right as an accredited data recipient*, https://www.linkedin.com/posts/acccgovau_become-an-accredited-data-recipientconsumer-activity-7008996803119390721-jOWF (accessed 16 December 2022).

—— 2022c, *Communique - Digital Platforms Regulators Forum*, https://www.accc.gov.au/update/communique-digital-platforms-regulators-forum (accessed 29 June 2022).

—— 2022d, *Digital platform services inquiry: Interim report No. 5 – Regulatory reform*, https://www.accc.gov.au/system/files/Digital%20platform%20services%20inquiry%20-%20September%202022%20interim%20report.pdf (accessed 10 December 2022).

—— 2022e, *Infrastructure record keeping rules: Project overview*, https://www.accc.gov.au/regulated-infrastructure/communications/monitoring-reporting/infrastructure-record-keeping-rules (accessed 13 May 2022).

—— 2022f, *Internet Activity Report: For the period ending 30 June 2022*, 5 December, https://www.accc.gov.au/regulated-infrastructure/telecommunications-and-internet/telecommunications-industry-record-keeping-and-reporting-rules/internet-activity-record-keeping-rule/june-2022-report (accessed 8 December 2022).

—— 2022g, *Measuring Broadband Australia - Report 17, June 2022*, Report 17, June, prepared by SamKnows.

—— 2022h, *Mobile Infrastructure Report 2022*, September, https://www.accc.gov.au/system/files/Mobile%20Infrastructure%20Report%202022.pdf (accessed 8 December 2022).

—— 2022i, *Scamwatch*, https://www.scamwatch.gov.au/ (accessed 7 July 2022).

Accenture 2021, *Consumer affordability of NBN services*, September.

—— 2022, *Cyber Threat Intelligence Report - volume 2 - 2021*.

ACMA (Australian Communications and Media Authority) 2021a, *About the Regional Broadband Scheme*, https://www.acma.gov.au/about-regional-broadband-scheme (accessed 15 June 2022).

—— 2021b, *Starlink Licence Details*, https://web.acma.gov.au/rrl/licence_search.licence_lookup?pLICENCE_NO=11181002/2 (accessed 13 May 2022).

ACOSS (Australian Council of Social Service) 2016, *Staying connected: the impact of digital exclusion on people living on low-incomes and the community organisations that support them*, January.

ACS (Australian Computer Society) 2020, *ACS Australia's Digital Pulse: Unlocking the potential of Australia's technology workforce*, Deloitte Access Economics, Sydney.

—— 2021a, *ACS Australia's Digital Pulse: Future directions for Australia's Technology workforce*, Deloitte Access Economics, Sydney.

—— 2021b, *Demand & Impacts on Tech & Digital Skills*, August.

—— 2021c, *The Ethics and Risks of AI Decision-Making*, June.

ACSC (Australian Cyber Security Centre) 2020, *Step-by-step guides*, https://www.cyber.gov.au/acsc/individuals-and-families/step-by-step-guides (accessed 25 May 2022).

—— 2021a, *ACSC Annual Cyber Threat Report: 1 July 2020 to 30 June 2021*.

—— 2021b, *Cyber Supply Chain Risk Management*, https://www.cyber.gov.au/acsc/view-all-content/publications/cyber-supply-chain-risk-management (accessed 1 June 2022).

—— 2021c, *Essential Eight*, https://www.cyber.gov.au/acsc/view-all-content/essential-eight (accessed 25 May 2022).

—— 2021d, *Ransomware Attacks: Emergency Response Guide*.

—— 2022a, *ACSC Annual Cyber Threat Report: July 2021 to June 2022*, https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-july-2021-june-2022 (accessed 8 December 2022).

—— 2022b, *Information Security Manual*, 10 March.

ADHA (Australian Digital Health Agency) 2021, *ePIP Conformance Register*, https://www.digitalhealth.gov.au/sites/default/files/documents/epip-conformance-register.pdf (accessed 6 December 2022).

—— 2022, *My Health Record: Statistics and Insights*, https://www.digitalhealth.gov.au/initiatives-and-programs/my-health-record/statistics (accessed 16 May 2022).

—— nd, *ePIP incentive eligibility requirements*, https://myhealthrecord.gov.au/for-healthcare-professionals/epip-incentive-eligibility-requirements (accessed 6 December 2022).

ADII (Australian Digital Inclusion Index) 2021, *Case study: Taking a deep dive into Digital Ability*.

—— 2022, *Explore the interactive data dashboards*, https://www.digitalinclusionindex.org.au/interactive-data-dashboards/ (accessed 18 May 2022).

Agarwal, A., Singhal, C. and Thomas, R. 2021, *AI-powered decision making for the bank of the future*, McKinsey & Company.

AGD (Attorney-General's Department) 2021, *Privacy Act Review: Discussion Paper*, October.

—— nd, *Protective Security Policy Framework*, https://www.protectivesecurity.gov.au/ (accessed 1 June 2022).

Aleisa, N., Renaud, K. and Bongiovanni, I. 2020, 'The privacy paradox applies to IoT devices too: A Saudi Arabian study', Elsevier, *Computers & Security*, vol. 96, p. 101897.

Alismaili, S.Z., Li, M., Shen, J., Huang, P., He, Q. and Zhan, W. 2020, 'Organisational-level assessment of cloud computing adoption: Evidence from the Australian SMEs', *Journal of Global Information Management*, vol. 28, no. 2, pp. 73–89.

AlphaBeta 2019a, *Australia's Digital Opportunity: Growing A $122 Billion A Year Tech Industry*, September.

—— 2019b, *Speed Check: Calibrating Australia's broadband speeds*, October.

Andal, S., Brown, A.-L., Grobler, D.M. and Richelle, R. 2022, *Small but stronger: Lifting SME cyber security in South Australia*, CSCRC, CSIRO's Data61, CyberCX.

Antonelli, W. 2022, 'What's a good internet speed? How to upgrade your internet setup to fit your needs', *Business Insider*.

APRA (Australian Prudential Regulation Authority) 2019, *Prudential Standard CPS 234: Information Security*, July.

ASD (Australian Signals Directorate) 2021, *Australian Signals Directorate Annual Report 2020–21: Key Activity 2 Cyber security services*, September.

Atlassian 2022, *Our distributed workforce*, https://www.atlassian.com/practices/use-cases/team-anywhere (accessed 18 May 2022).

ATO (Australian Taxation Office) 2019, *Digital Partnership Office (DPO)*, https://softwaredevelopers.ato.gov.au/DPO (accessed 16 May 2022).

—— 2021a, *Micro employers*, https://www.ato.gov.au/business/single-touch-payroll/concessional-reporting/micro-employers/ (accessed 16 June 2022).

—— 2021b, *Seasonal and intermittent employers*, https://www.ato.gov.au/Business/Single-Touch-Payroll/In-detail/Seasonal-and-intermittent-employers/ (accessed 16 June 2022).

—— 2021c, *Single Touch Payroll*, https://www.ato.gov.au/business/single-touch-payroll/ (accessed 16 June 2022).

—— 2022, *Product Register*, https://softwaredevelopers.ato.gov.au/product-register#Functionality=*Payroll%20(STP) (accessed 17 May 2022).

Attwooll, J. 2022, *Pandemic prompts massive spike in My Health Record use*, https://www1.racgp.org.au/newsgp/professional/pandemic-prompts-massive-spike-in-my-health-record (accessed 5 December 2022).

AustCyber 2020, *Australia's Cyber Security Sector Competitiveness Plan 2020*, 29 November.

Australian Government 2015, *The cost of cybercrime to Australia*, https://www.infrastructure.gov.au/sites/default/files/Cost%20of%20cybercrime_INFOGRAPHIC_WEB_published_08102015.pdf (accessed 7 July 2022).

—— 2021a, *Consumer Data Right: Phasing in the banking sector*, https://www.cdr.gov.au/sites/default/files/2021-08/CDR-Phasinginthebankingsector.pdf (accessed 30 May 2022).

—— 2021b, *Mobile Blackspot Database*, https://data.gov.au/dataset/ds-nsw-4b681b2d-d7aa-4d60-94ee-bea51e52b82d/details?q=mobile%20black%20spot (accessed 13 May 2022).

—— 2022, *Consumer Data Right: Performance*, https://www.cdr.gov.au/performance (accessed 4 July 2022).

—— nd, *Where to use it*, myGovID, https://www.mygovid.gov.au/where-to-use (accessed 24 November 2022).

Awad, E., Dsouza, S., Kim, R., Schulz, J., Henrich, J., Shariff, A., Bonnefon, J.-F. and Rahwan, I. 2018, 'The moral machine experiment', *Nature*, vol. 563, no. 7729, pp. 59–64.

AWS 2022, *AWS Certification*, https://aws.amazon.com/certification/ (accessed 17 May 2022).

Barbaschow, A. 2021a, 'Critical infrastructure Bill has a government "step in" powers labelling problem', *ZDNet*.

—— 2021b, 'Logistics and utilities providers agree to help from ASD in the event of a cyber incident', *ZDNet*.

Barth, S. and De Jong, M.D. 2017, 'The privacy paradox–Investigating discrepancies between expressed privacy concerns and actual online behavior–A systematic literature review', Elsevier, *Telematics and informatics*, vol. 34, no. 7, pp. 1038–1058.

Basu, S., Fernald, J.G. and Kimball, M.S. 2006, 'Are technology improvements contractionary?', *American Economic Review*, vol. 96, no. 5, pp. 1418–1448.

BCARR (Bureau of Communications, Arts and Regional Research) 2021, *Working paper - Economic impact of ubiquitous high speed broadband: agriculture sector*, May, Commonwealth of Australia, Canberra, ACT.

Beaunoyer, E., Dupéré, S. and Guitton, M. 2020, 'COVID-19 and digital inequalities: Reciprocal impacts and mitigation strategies', *Computers in Human Behavior*, vol. 111, October 2020, p. 106424.

Bennett, T. and Davidson, J. 2022, *Government pushes for digital identity system after Optus hack*, Australian Financial Review, https://www.afr.com/technology/government-pushes-

for-digital-identity-system-after-optus-hack-20220928-p5blrf (accessed 24 November 2022).

Blackburn, S., Freeland, M. and Gärtner, D. 2017, *Digital Australia: Seizing opportunities from the Fourth Industrial Revolution*, March, McKinsey & Company, Sydney.

Blease, C., Torous, J. and Hägglund, M. 2020, 'Does patient access to clinical notes change documentation?', Frontiers Media SA, *Frontiers in Public Health*, vol. 8, p. 577896.

Bloom, N., Sadun, R. and Reenen, J.V. 2012, 'Americans do it better: US multinationals and the productivity miracle', *American Economic Review*, vol. 102, no. 1, pp. 167–201.

BoCAR (Bureau of Communications and Arts Research) 2020, *Demand for fixed-line broadband in Australia 2018–2028: Working Paper*, July, Department of Industry, Science, Energy and Resources, Commonwealth of Australia, Canberra.

Bongiovanni, I., Renaud, K. and Aleisa, N. 2020, *The privacy paradox: we claim we care about our data, so why don't our actions match?*, The Conversation, http://theconversation.com/the-privacy-paradox-we-claim-we-care-about-our-data-so-why-dont-our-actions-match-143354 (accessed 16 December 2022).

Borowiecki, M., Pareliussen, J., Glocker, D., Kim, E.J., Polder, M. and Rud, I. 2021, *The Impact of Digitalisation on Productivity: Firm-Level Evidence from the Netherlands*, OED Economics Department Working Papers, No. 1680, 9 August, OECD Publishing, Paris.

Bova, F., Goldfarb, A. and Melko, R. 2021, 'Quantum Computing Is Coming. What Can It Do?', *Harvard Business Review*.

Bowman, K. and Callan, V.J. 2021, *Engaging More Employers in Nationally Recognised Training to Develop their Workforce*, National Centre for Vocational Education Research, Adelaide.

Boyd, T. 2021, 'NBN's monopoly getting stronger', *Australian Financial Review*, 29 April.

Boyton, A. 2022, *Australian Business Economists Speech by the National Skills Commissioner*, 14 February.

Braue, D. 2022, '4 in 10 CISOs unprepared to stop attacks', *Information Age*, 17 May.

Brennan, M. 2021, *Reform and Sustainable Funding of Healthcare*, Productivity Commission Chairman's Speech, 3 August, Healthcare Leaders Forum.

Bresnahan, T.F. and Trajtenberg, M. 1995, 'General purpose technologies "Engines of growth"?', Elsevier, *Journal of Econometrics*, vol. 65, no. 1, pp. 83–108.

Brynjolfsson, E. and Hitt, L.M. 2000, 'Beyond computation: Information technology, organizational transformation and business performance', *Journal of Economic perspectives*, vol. 14, no. 4, pp. 23–48.

Buckley, R.P., Jevglevskaja, N. and Farrell, S. 2022, 'Australia's data-sharing regime: Six lessons for Europe', *King's Law Journal*, vol. 33, no. 1, pp. 61–91.

Burns, D. 2022, *Our role connecting millions of Australians from space*, 2 February, Telstra.

Burton, T. 2022a, *Digital Transformation Agency plots a new path to help build digital government*, Australian Financial Review, https://www.afr.com/politics/federal/digital-transformation-agency-plots-a-new-path-20221006-p5bnp6 (accessed 24 November 2022).

—— 2022b, 'New myGov app to be platform for public and private services', *Australian Financial Review*, 5 December, https://www.afr.com/politics/federal/new-mygov-app-to-be-platform-for-public-and-private-services-20221205-p5c3od (accessed 5 December 2022).

Cabinet Office 2022, *Government Cyber Security Strategy: 2022 to 2030*, 17 February.

California Policy Lab nd, *What we do*, https://www.capolicylab.org/what-we-do/ (accessed 16 May 2022).

Catania, P., Wheelahan, F. and Mani, K. 2022, *New public sector data sharing laws: key considerations for the private sector*, https://www.corrs.com.au/insights/new-public-sector-data-sharing-laws-key-considerations-for-the-private-sector (accessed 27 May 2022).

CBA (Commonwealth Bank of Australia) 2022, *Bill Sense*, https://www.commbank.com.au/digital-banking/bill-sense.html (accessed 18 May 2022).

CDDO (Central Digital and Data Office) 2020, *Data Ethics Framework*, https://www.gov.uk/government/publications/data-ethics-framework/data-ethics-framework-2020 (accessed 1 June 2022).

CEDA 2017, *Australians acting in a contradictory manner with data privacy*, https://www.ceda.com.au/NewsAndResources/News/Data-Digital-economy/Australians-acting-in-a-contradictory-manner-with (accessed 16 December 2022).

—— 2022, *AI Principles to Practice*.

Chakravorti, B., Bhalla, A. and Chaturvedi, R.S. 2019, 'Which Countries Are Leading the Data Economy?', *Harvard Business Review*.

Chatwood, R. and Allen, B. 2019, *Australia suddenly passes new laws regulating streaming of abhorrent violent material by ISPs and other content providers*, https://www.dentons.com/en/insights/alerts/2019/april/15/australia-suddenly-passes-new-laws-regulating-streaming-of-abhorrent-violent-material (accessed 31 May 2022).

Cheu, S. 2021, 'Aged care provider uptake of My Health Record remains low', *Australian Ageing Agenda*.

Christie, A. and Wong, J. 2021, *Australian governments agree to sharing of public sector data between them as 'default position'*, 27 July, Clyde & Co.

Chui, M., Farrell, D. and Jackson, K. 2014, How Government can promote open data and help unleash over $3 trillion in economic value, McKinsey, 1 April.

CISC (Cyber and Infrastructure Security Centre) 2022a, *Cyber Security Incident Reporting*, April.

—— 2022b, *Legislative information and reforms: Critical infrastructure*, https://www.cisc.gov.au/legislative-information-and-reforms/critical-infrastructure (accessed 3 June 2022).

Cisco 2022, *Cisco Certifications*, https://www.cisco.com/c/en/us/training-events/training-certifications/certifications.html (accessed 17 May 2022).

Clark, J. 2016, *What is the Internet of Things (IoT)?*, https://www.ibm.com/blogs/internet-of-things/what-is-the-iot/ (accessed 15 June 2022).

CMA (Competition and Markets Authority) 2021, *A joined-up approach to digital regulation: Digital Regulation Cooperation Forum publishes its first annual plan of work*, 10 March.

CompTIA 2020, *The Role of Emerging Technology in Digital Transformation*, CompTIA Worldwide Headquarters, Chicago, Illinois.

Coursera 2021, *Google launches three new entry-level Professional Certificates on Coursera*, https://blog.coursera.org/

google-launches-three-new-entry-level-professional-certificates-on-coursera/ (accessed 27 July 2022).

Coyle, D. and Manley, A. 2022, *What is the Value of Data? A review of empirical methods*, July, Bennett Institute for Public Policy, Cambridge.

CPA Australia 2021, *Business Technology Report 2021*.

Crozier, R. 2021, 'HyperOne to deploy $1.5bn, 20,000 km fibre backbone across Australia', *IT News*.

CRTC (Canadian Radio-television and Telecommunications Commission) 2020, *Measuring Broadband Canada Project*, https://crtc.gc.ca/eng/internet/proj.htm (accessed 6 June 2022).

CyberEdge 2021, *2021 Cyberthreat Defense Report*, CyberEdge Group.

—— 2022, *2022 Cyberthreat Defense Report*, CyberEdge Group, https://cyber-edge.com/cdr/ (accessed 8 December 2022).

Cynch Security, Deakin University, RMIT University and AustCyber 2021, *Big cyber security questions for small business: The state of cyber fitness in Australian small businesses*, Cynch Security, Melbourne.

DAE (Deloitte Access Economics) 2019a, *Benefits of small business digital engagement*.

—— 2019b, *The Economic Value of Cloud Services in Australia*.

Data Republic 2020, *Inquiry into Future Directions for the Consumer Data Right*, April.

Davenport, T.H. and Mittal, N. 2020, 'How CEOs Can Lead a Data-Driven Culture', *Harvard Business Review*.

DAWE (Department of Agriculture, Water and the Environment) 2022, *Food Safety Recognition Agreements (Arrangements) with other countries*, https://www.awe.gov.au/biosecurity-trade/export/from-australia/food-safety-recognition-agreements (accessed 27 June 2022).

Dawson, D., Schleiger, E., Horton, J., McLaughlin, J., Robinson, C., Quezada, G., Scowcroft, J. and Hajkowicz, S. 2019, *Artificial intelligence: Australia's ethics framework-a discussion paper*, Data61 CSIRO.

DCA (Department of Communications and the Arts) 2018, *Development of the Universal Service Guarantee: Summary Report*, November.

DeakinCo and Deloitte Access Economics 2022, *The Business Return On Learning And Development*, March, Deakin University, Melbourne.

Defence (Department of Defence) 2020, *Nation's largest ever investment in cyber security*, 30 June.

DeFilippis, E., Impink, S.M., Singell, M., Polzer, J.T. and Sadun, R. 2020, *Collaborating during coronavirus: The impact of COVID-19 on the nature of work*, Working Paper 27612, National Bureau of Economic Research, United States.

Deloitte Insights 2019, *Future in the balance? How countries are pursuing an AI advantage*, Deloitte Center For Technology, Media & Telecommunications, New York.

Delua, J. 2021, *Supervised vs. Unsupervised Learning: What's the Difference?*, https://www.ibm.com/cloud/blog/supervised-vs-unsupervised-learning (accessed 1 June 2022).

Department of Health 2019, *Practice Incentives Program Quality Improvement Incentive Guidelines*.

DESE (Department of Education, Skills and Employment) 2021, *Higher Education Data Cube (uCube)*, http://highereducationstatistics.education.gov.au/ (accessed 8 June 2022).

—— 2022, *Award Course Completions Pivot Table*, https://www.dese.gov.au/higher-education-statistics/resources/award-course-completions-pivot-table (accessed 8 June 2022).

DISER (Department of Industry, Science, Energy and Resources) 2021, *Cyber Security Assessment Tool*, https://digitaltools.business.gov.au/jfe/form/SV_0dnd9cF15I8LnH8?ref=bga (accessed 28 June 2022).

—— nd, *Australia's Artificial Intelligence Ethics Framework: Testing the AI Ethics Principles*, https://www.industry.gov.au/data-and-publications/australias-artificial-intelligence-ethics-framework/testing-the-ai-ethics-principles (accessed 1 June 2022).

DISR (Department of Industry, Science, and Resources) 2019, *Australia's Artificial Intelligence Ethics Framework*, https://www.industry.gov.au/data-and-publications/australias-artificial-intelligence-ethics-framework (accessed 1 June 2022).

DITRDC (Department of Infrastructure, Transport, Regional Development and Communications) 2019, *Regional Tech Hub*, www.infrastructure.gov.au/media-technology-communications/internet/regional-tech-hub (accessed 8 June 2022).

—— 2020, *NBN - Fixed-wireless*, https://data.gov.au/data/dataset/national-broadband-network-connections-by-technology-type/resource/5230f085-2395-4e6e-8d4f-fc7721fb5510 (accessed 2 June 2022).

—— 2021a, *Mobile Black Spot Program*, https://www.infrastructure.gov.au/media-technology-communications/phone/mobile-services-coverage/mobile-black-spot-program (accessed 12 May 2022).

—— 2021b, *Universal Service Guarantee – fact sheet*, 3 September.

—— 2022a, *NBN fixed wireless receives major budget boost*, https://www.infrastructure.gov.au/department/media/news/nbn-fixed-wireless-receives-major-budget-boost (accessed 13 May 2022).

—— 2022b, *Regional Connectivity Program*, https://www.infrastructure.gov.au/media-communications-arts/internet/regional-connectivity-program (accessed 12 May 2022).

—— 2022c, *Spectrum allocations*, https://www.infrastructure.gov.au/media-communications-arts/spectrum/spectrum-allocations (accessed 26 July 2022).

DJPR (Victorian Department of Jobs, Precincts and Regions) 2022, *Digital Jobs: Building Victoria's digital workforce*, https://djpr.vic.gov.au/digital-jobs (accessed 8 June 2022).

DLA Piper 2022, *Breach Notification: United States*, https://www.dlapiperdataprotection.com/index.html?t=breach-notification&c=US (accessed 1 June 2022).

Dobscha, S.K., Denneson, L.M., Jacobson, L.E., Williams, H.B., Cromer, R. and Woods, S. 2016, 'VA mental health clinician experiences and attitudes toward OpenNotes', Elsevier, *General hospital psychiatry*, vol. 38, pp. 89–93.

Domeyer, A., Hieronimus, S., Klier, J. and Weber, T. 2021, *Government data management for the digital age*, 20 September, McKinsey & Company.

DP-REG (Digital Platform Regulators Forum) 2022, *Digital Platform Regulators Forum (DP-REG): Terms of Reference*, March.

DRCF (Digital Regulation Cooperation Forum) 2022, *Digital Regulation Cooperation Forum: Annual report 2021 to 2022*, 28 April.

DSO (Digital Skills Organisation) 2021, *Projects: Train 100 Data Analysts*, https://digitalskillsorg.com.au/t100/ (accessed 8 June 2022).

DSS (Department of Social Services) 2021, *Be Connected – improving digital literacy for older Australians*, https://www.dss.gov.au/seniors/be-connected-improving-digital-literacy-for-older-australians (accessed 8 June 2022).

DTA (Digital Transformation Agency) 2021, *Hardening Government IT (HGIT) Initiative*, https://www.dta.gov.au/our-projects/hardening-government-it-hgit-initiative (accessed 1 June 2022).

—— 2022a, *Digital Identity Legislation Background Paper*, Digital Identity Australian Government, https://digitalidentity.gov.au (accessed 24 November 2022).

—— 2022b, *Trusted Digital Identity Framework (TDIF)*, Digital Identity Australian Government, https://www.digitalidentity.gov.au/tdif (accessed 24 November 2022).

—— nd, *Digital Service Standard criteria: 5. Make it secure*, https://www.dta.gov.au/help-and-advice/digital-service-standard/digital-service-standard-criteria/5-make-it-secure (accessed 1 June 2022).

Duch-Brown, N., Martens, B. and Mueller-Langer, F. 2017, *The Economics of Ownership, Access and Trade in Digital Data*, JRC Digital Economy Working Paper 2017-01, European Commission.

EC (European Commission) 2021a, *Broadband Coverage in Europe 2013-2020*, https://ec.europa.eu/newsroom/dae/redirection/document/80627 (accessed 6 June 2022).

—— 2021b, *Ethics By Design and Ethics of Use Approaches for Artificial Intelligence*, 25 November.

—— 2021c, *Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*.

—— 2022, *Shaping Europe's digital future: Regulatory framework proposal on artificial intelligence*, https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai (accessed 1 June 2022).

Eggers, W., Turley, M. and Kishnani, P.K. 2018, *The future of regulation Principles for regulating emerging technologies*, 19 June, Deloitte Insights.

EIPA (European Institute of Public Administration) 2021, *The Artificial Intelligence Act Proposal and its Implications for Member States*, https://www.eipa.eu/publications/briefing/the-artificial-intelligence-act-proposal-and-its-implications-for-member-states/ (accessed 1 June 2022).

Eitel-Porter, R. 2021, 'Beyond the promise: implementing ethical AI', *AI and Ethics*, vol. 1, no. 1, pp. 73–80.

Estcourt, D. and Eddie, R. 2022, '"Absolute authority": Call to halt plan to collect all Victorians' medical records', *The Age*, 11 March.

Eyers, J. 2022a, 'ACCC warns banks on delivery of consumer data right', *Australian Financial Review*, 2 June.

—— 2022b, 'Banks will use open data to assess loans this year', *Australian Financial Review*, 11 April.

Farrell, S. 2020, *Future Directions for the Consumer Data Right*, October, Commonwealth of Australia, Canberra.

FCA (Federal Court of Australia) 2022, *Australian Securities and Investments Commission v RI Advice Group Pty (Judgement Summaries)*, 5 May.

FCC (Federal Communications Commission) 2021, *Measuring Fixed Broadband - Eleventh Report*, 31 December.

—— 2022, *Chairwoman Rosenworcel Proposes To Increase Minimum Broadband Speeds And Set Gigabit Future Goal*, Media release, 15 July.

Featherstone, D., Ormond-Parker, L. and Holcombe-James, I. 2022, *Mapping the Digital Gap: Wilcannia NSW Community Outcomes report 2022*, June, ARC Centre of Excellence for Automated Decision Making and Society: RMIT University, Melbourne.

Fifth Quadrant, Ethical AI Advisory and Gradient Institute 2021, *Responsible AI Index Report*.

Fogg, B. 2022, *Starlink in Australia: SpaceX's satellite internet explained*, https://www.reviews.org/au/internet/starlink-satellite-internet-australia/ (accessed 13 May 2022).

Forrest, C. 2017, *66% of SMBs would shut down or close if they experienced a data breach*, https://www.techrepublic.com/article/66-of-smbs-would-shut-down-or-close-if-they-experienced-a-data-breach/ (accessed 7 July 2022).

Francom, S.R. 2020, *How Fast Should My Business Internet Be?*, https://www.business.org/services/internet/business-internet-speed/ (accessed 20 May 2022).

Gal, P., Nicoletti, G., Renault, T., Sorbe, S. and Timiliotis, C. 2019, *Digitalisation and productivity: In search of the holy grail – Firm-level empirical evidence from EU countries*, OECD Economics Department Working Papers 1533, 12 February.

Gartner 2021, *Gartner Survey Reveals Talent Shortages as Biggest Barrier to Emerging Technologies Adoption*, 13 September, Stamford, Conn.

General Assembly 2022, *Course Catalog*, https://generalassemb.ly/browse?format=all (accessed 17 May 2022).

Gillespie, N., Lockey, S. and Curtis, C. 2020, *Trust in Artificial Intelligence: Australian Insights*, The University of Queensland and KPMG Australia.

Gillezeau, N. 2020, 'The quietly rising power of product managers', *Australian Financial Review*, 2 December.

Goldfarb, A. and Tucker, C. 2019, 'Digital economics', *Journal of Economic Literature*, vol. 57, no. 1, pp. 3–43.

GovLab 2017a, *California Policy Lab (CPL)*, https://medium.com/data-labs/california-policy-lab-cpl-b926603765dc (accessed 16 May 2022).

—— 2017b, *Ministry of Justice Data Lab*, https://medium.com/data-labs/ministry-of-justice-data-lab-8d8b0779c295 (accessed 16 May 2022).

Govtech Review 2021, 'Public sector IT spend to grow 8.8% in 2022'.

Griffith, C. 2022, 'Telstra, OneWeb in deal on satellites', *The Australian*, 2 March.

Gutierrez, A., Boukrami, E. and Lumsden, R. 2015, 'Technological, organisational and environmental factors influencing managers' decision to adopt cloud computing in the UK', *Journal of Enterprise Information Management*, vol. 28, no. 6, pp. 788–807.

Haeck, P. 2021, 'Ex-Google boss slams transparency rules in Europe's AI bill', *Politico*.

Hambur, J., Montaigne, M., Parsons, S. and Whalan, E. 2022, *Looking Under the Lamppost or Shining a New Light: New Data for Unseen Challenges*, February, p. 15.

Havard, V., Jeanne, B., Lacomblez, M. and Baudry, D. 2019, 'Digital twin and virtual reality: a co-simulation environment for design and assessment of industrial workstations', *Production and Manufacturing Research*, vol. 7, no. 1, pp. 472–489.

Health Metrics 2021, *Interoperable Software Key to Uptake of My Health Record*, https://healthmetrics.com.au/my-health-record-aged-care/ (accessed 16 May 2022).

Hendrie, D. 2019, 'Is My Health Record becoming useful to GPs?', *News GP*.

Hendry, J. 2022, *Digital ID could prevent Optus breach repeat: Home Affairs*, InnovationAus.com, https://www.innovationaus.com/digital-id-could-prevent-optus-breach-repeat-home-affairs/ (accessed 24 November 2022).

Hirschhorn, J. 2021, *Digital transformation – Australia as a world leader*, 1 September.

Home Affairs (Department of Home Affairs) 2020a, Australia's Cyber Security Strategy 2020.

—— 2020b, *Protecting Critical Infrastructure and Systems of National Significance: Consultation Paper*, August.

—— 2021a, *2020 – 21 Migration Program Report: Program year to 30 June 2021*.

—— 2021b, *Ransomware Action Plan*.

—— 2021c, *Skilled occupation list*, https://immi.homeaffairs.gov.au/visas/working-in-australia/skill-occupation-list (accessed 24 February 2022).

—— 2021d, *Temporary Skill Shortage visa*, https://immi.homeaffairs.gov.au/visas/getting-a-visa/visa-listing/temporary-skill-shortage-482 (accessed 18 May 2022).

—— 2021e, *Visas for innovation: Global Talent Employer Sponsored program*, https://immi.homeaffairs.gov.au/visas/working-in-australia/visas-for-innovation/global-talent-scheme (accessed 18 May 2022).

—— 2021f, *Visas for innovation: Global Talent Visa Program*, https://immi.homeaffairs.gov.au/visas/working-in-australia/visas-for-innovation/global-talent-independent-program (accessed 18 May 2022).

—— 2022a, *Engagement on critical infrastructure reforms*, https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/protecting-our-critical-infrastructure-reforms-engagement (accessed 25 May 2022).

—— 2022b, *Nominating a position: List of current labour agreements*, https://immi.homeaffairs.gov.au/visas/employing-and-sponsoring-someone/sponsoring-workers/nominating-a-position/labour-agreements/list-of-current-labour-agreements (accessed 18 May 2022).

Huang, K., Pearlson, K. and Madnick, S. 2021, 'Is Third-Party Software Leaving You Vulnerable to Cyberattacks?', *Harvard Business Review*.

Huawei and Oxford Economics 2017, *Digital Spillover: Measuring the true impact of the digital economy*.

IA (Infrastructure Australia) 2022a, *Delivering Outcomes: A roadmap to improve infrastructure industry productivity and innovation*, March.

—— 2022b, *Regional Strengths and Infrastructure Gaps*, March.

—— 2022c, *Regional Strengths and Infrastructure Gaps: Interactive Map*, https://www.infrastructureaustralia.gov.au/regional-strengths-map (accessed 7 July 2022).

IBM 2021, *Cost of a Data Breach Report 2021*, July, IBM Corporation, Armonk, NY.

—— nd, *What is blockchain technology?*, https://www.ibm.com/au-en/topics/what-is-blockchain (accessed 15 June 2022a).

—— nd, *What is quantum computing?*, https://www.ibm.com/topics/quantum-computing (accessed 18 May 2022b).

IDCARE 2022, *IDCARE Subscriber Organisations*, https://www.idcare.org/about-idcare/our-subscribing-organisations (accessed 7 July 2022).

Internet Australia 2021, *Submission to the Regional Telecommunications Review 2021*, 30 September.

Jackson, K. 2000, *The Telecommunications Universal Service Obligation (USO)*, https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/Publications_Archive/archive/uso (accessed 14 June 2022).

Jouanjean, M.-A., Casalini, F., Wiseman, L. and Gray, E. 2020, *Issues around data governance in the digital transformation of agriculture: The farmers' perspective*, 23 October, OECD Food, Agriculture and Fisheries Papers, OECD Publishing, Paris.

Karen, S. 2021, 'Govt urged to pass infrastructure cyber security intervention powers', *ARNnet*.

Kox, H. and Straathof, B. 2014, *Economic aspects of Internet security*, CPB Background Document, Central Planning Bureau, Netherlands.

Kwan, C. 2021, 'Critical Infrastructure Bill should be split to swiftly give government step-in powers: PJCIS', *ZDNet*.

—— 2022, *Planning for telecommunications CDR rules and open finance are underway*, https://www.zdnet.com/article/telecommunications-sector-officially-designated-for-cdr-and-open-finance-is-underway/ (accessed 30 May 2022).

Lambert, T. 2021, 'What's behind the war on big tech?', *Regulation*, vol. Fall 2021, pp. 30–36.

Lim, C., Bowe, K., Gunning, P. and Denham, C. 2022, *Parliament Considers Ransomware Plan Legislation*, https://www.kwm.com/au/en/insights/latest-thinking/parliament-considers-ransomware-plan-details.html (accessed 25 May 2022).

Lipsey, R.G., Carlaw, K.I. and Bekar, C.T. 2005, *Economic transformations: general purpose technologies and long-term economic growth*, Oxford University Press, Oxford.

Manyika, J., Silberg, J. and Presten, B. 2019, 'What Do We Do About the Biases in AI?', *Harvard Business Review*.

MCA (Minerals Council of Australia) 2022, *The Digital Mine: A review of Australia's mining innovation ecosystem*, September, https://www.minerals.org.au/sites/default/files/The%20Digital%20Mine_2022.pdf (accessed 10 January 2023).

McKinsey 2019, *Catch them if you can: How leaders in data and analytics have pulled ahead*, 19 September.

Medibank 2022, *Calvary-Medibank using AI and remote monitoring to support more than 130,000 COVID patients so far*, https://www.medibank.com.au/livebetter/newsroom/post/calvary-medibank-using-ai-and-remote-monitoring-to-support-more-than-130-000 (accessed 9 August 2022).

Microsoft 2019, *Microsoft and General Assembly launch partnership to close the global AI skills gap*, https://news.microsoft.com/2019/05/17/microsoft-and-general-assembly-launch-partnership-to-close-the-global-ai-skills-gap/ (accessed 27 July 2022).

—— 2022, *Browse Certifications and Exams*, https://docs.microsoft.com/en-us/learn/certifications/browse/ (accessed 17 May 2022).

Min, H. 2000, 'Electronic data interchange in supply chain management', in Swamidass, P. (ed), *Encyclopedia of Production and Manufacturing Management*, Springer, Boston, MA.

MoJ (Ministry of Justice) 2018, *Accessing the Justice Data Lab service*, https://www.gov.uk/government/publications/justice-data-lab (accessed 16 May 2022).

Moll, J. and Cajander, Å. 2020, 'Oncology health-care professionals' perceived effects of patient accessible electronic health records 6 years after launch: a survey study at a major university hospital in Sweden', SAGE Publications Sage UK: London, England, *Health informatics journal*, vol. 26, no. 2, pp. 1392–1403.

Moore, T. 2010, 'The economics of cybersecurity: Principles and policy options', Elsevier, *International Journal of Critical Infrastructure Protection*, vol. 3, no. 3–4, pp. 103–117.

Müller, V. 2020, *Ethics of Artificial Intelligence and Robotics*, 30 April, Stanford Encyclopedia of Philosophy.

MYOB 2022, *The Digital Disconnection Challenge*, June, https://www.myob.com/content/dam/public-website/docs/misc/The%20Digital%20Disconnection%20Challenge_MYOB%20Report%202022.pdf (accessed 22 November 2022).

National Cabinet 2021, *Intergovernmental Agreement on data sharing between Commonwealth and State and Territory governments*, July.

NBN 2020, *Initial build complete, NBN Co announces next phase of network investment to meet future demand*, https://www.nbnco.com.au/content/dam/nbnco2/2020/documents/media-centre/corporate-plan-2021/nbnco-media-release-corporate-plan-2021.pdf (accessed 12 May 2022).

—— 2022, *The technology that connects your premises*, https://www.nbnco.com.au/learn/network-technology (accessed 5 May 2022).

NCVER (National Centre for Vocational Education Research) 2021, *Employers' Use and Views of the VET System 2021*.

—— 2022, *VOCSTATS*, https://www.ncver.edu.au/research-and-statistics/vocstats (accessed 17 May 2022).

NDIA (National Disability Insurance Agency) 2020, *Delivering the NDIS: Digital Partnership Program begins developer onboarding phase*, https://www.ndis.gov.au/news/4887-delivering-ndis-digital-partnership-program-begins-developer-onboarding-phase (accessed 14 June 2022).

NIST (National Institute of Standards and Technology) 2022, *Software Supply Chain Security Guidance Under Executive Order (EO) 14028 Section 4e*, 4 February.

NSC (National Skills Commission) 2021a, *Skills Priority List*, https://www.nationalskillscommission.gov.au/topics/skills-priority-list (accessed 31 May 2022).

—— 2021b, *Skills Priority List Findings: ICT Professionals*, National Skills Commission, Canberra.

—— 2022, *Australian Skills Classification 2.0 data*, https://www.nationalskillscommission.gov.au/sites/default/files/2022-03/Australian%20Skills%20Classification%20-%20March%202022.xlsx (accessed 31 May 2022).

—— nd, *Australian Skills Classification*, https://www.nationalskillscommission.gov.au/topics/australian-skills-classification (accessed 18 May 2022).

NSW Government 2021, *NSW Identity Strategy*, April, https://www.nsw.gov.au/sites/default/files/2021-05/NSW-Government-Identity-Strategy-accessible.pdf (accessed 24 November 2022).

NSW Health 2021, *Lumos: Shining a light on the patient journey in NSW*, https://www.health.nsw.gov.au/lumos (accessed 16 May 2022).

NSW PC (NSW Productivity Commission) 2022, *Adaptive NSW: how embracing tech could recharge our prosperity*, November, https://www.productivity.nsw.gov.au/sites/default/files/2022-11/20221117-nsw-productivity-commission_adaptive-nsw_how-embracing-tech-could-recharge-our-prosperity.pdf (accessed 28 November 2022).

OAIC (Office of the Australian Information Commissioner) 2017, *Australian Community Attitudes to Privacy Survey 2017*, Home, https://www.oaic.gov.au/updates/videos/australian-community-attitudes-to-privacy-survey-2017 (accessed 16 December 2022).

—— 2021, *Data breach report highlights ransomware and impersonation fraud as concerns*, 23 August.

—— nd, *About the Notifiable Data Breaches scheme*, https://www.oaic.gov.au/privacy/notifiable-data-breaches/about-the-notifiable-data-breaches-scheme (accessed 1 June 2022).

ODI (Open Data Institute) 2020, *The value of sharing data in supply chain optimisation*, 3 March.

OECD (Organisation for Economic Co-operation and Development) 2015, *Data-Driven Innovation: Big Data for Growth and Well-Being*, OECD Publishing, Paris.

—— 2019, *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*, 26 November, OECD Publishing, Paris.

—— 2020, *Shaping the Future of Regulators: The Impact of Emerging Technologies on Economic Regulators, The Governance of Regulators*, OECD Publishing, Paris.

—— 2021, *SMEs Going Digital: Policy challenges and recommendations*, Going Digital Toolkit Policy Note, 15.

—— 2022a, *Broadband Portal*, https://www.oecd.org/digital/broadband/broadband-statistics/ (accessed 20 May 2021).

—— 2022b, *ICT Access and Usage by Businesses*, https://stats.oecd.org/Index.aspx?DataSetCode=ICT_BUS (accessed 20 May 2022).

Ofcom (Office of Communications) 2022, *International Broadband Scorecard 2020: interactive data*, London, UK.

ONDC (Office of the National Data Commissioner) 2022, *Data Availability and Transparency Act 2022*, https://www.datacommissioner.gov.au/data-legislation/data-availability-and-transparency-act (accessed 13 May 2022).

Ookla Speedtest 2022, *Speedtest Global Index*, https://www.speedtest.net/global-index (accessed 2 February 2022).

OPCC (Office of the Privacy Commissioner of Canada) 2020, *A Regulatory Framework for AI: Recommendations for PIPEDA Reform*, November.

OPCNZ and CDS (Office of the Privacy Commissioner (New Zealand) and Chief Data Steward) 2018, *Principles for safe and effective use of data and analytics*,

https://www.privacy.org.nz/publications/guidance-resources/principles-for-the-safe-and-effective-use-of-data-and-analytics-guidance/ (accessed 1 June 2022).

Open Knowledge Foundation 2017, *Global Open Data Index: Australia*, https://index.okfn.org/place/au/ (accessed 13 May 2022).

Optus 2016, *Submission in Response to Productivity Commission Issues Paper: Telecommunications Universal Service Obligation*, July.

Pagone, T. and Briggs, L. 2021, *Aged Care Royal Commission Final Report: Recommendations*.

Parliament of Australia 2022, *Crimes Legislation Amendment (Ransomware Action Plan) Bill 2022*.

Parliament of Victoria 2021, *Health Legislation Amendment (Information Sharing) Bill 2021*, 4 October.

PC (Australian Government Competitive Neutrality Complaints Office) 2022, *NBN Co*, Investigation No. 18, Canberra.

—— 2014, *Public Infrastructure*, Report no. 71, Canberra.

—— 2015, *Public Safety Mobile Broadband*, Research Report, Canberra.

—— 2016, *Intellectual Property Arrangements*, Report no. 78, Canberra.

—— 2017a, *Data Availability and Use*, Report no. 82, Canberra.

—— 2017b, *Telecommunications Universal Service Obligation*, Report no. 83, Canberra.

—— 2018, *Superannuation: Assessing Efficiency and Competitiveness*, Report no. 91, Canberra.

—— 2021a, *Australia's prison dilemma*, Research Paper, Canberra.

—— 2021b, *Innovations in Care for Chronic Health Conditions*, Productivity Reform Case Study, Canberra.

—— 2021c, *Working from home*, Commission Research Paper, Canberra.

Penn, A. 2021, *We're investing hundreds of millions to extend and enhance our regional, rural and remote coverage*, 6 May, Telstra.

Pérez, L., Rodríguez-Jiménez, S., Rodríguez, N., Usamentiaga, R. and García, D.F. 2020, 'Digital twin and virtual reality based methodology for multi-robot manufacturing cell commissioning', *Applied sciences*, vol. 10, no. 10, p. 3633.

Petersson, L., Erlingsdóttir, G., and others 2018, 'Open notes in Swedish psychiatric care (part 2): survey among psychiatric care professionals', JMIR Publications Inc., Toronto, Canada, *JMIR mental health*, vol. 5, no. 2, p. e10521.

PMC (Department of Prime Minister and Cabinet) 2021a, *Australian Data Strategy Action Plan*, Commonwealth of Australia, Canberra.

—— 2021b, *Australian Data Strategy: The Australian Government's whole-of-economy vision for data*, Commonwealth of Australia, Canberra.

—— 2021c, *Digital Economy Strategy 2030*, Commonwealth of Australia, Canberra.

—— 2022a, *$20 million investment in software to save businesses time and money*, https://ministers.pmc.gov.au/morton/2022/20-million-investment-software-save-businesses-time-and-money (accessed 16 May 2022).

—— 2022b, *Digital Economy Strategy 2022 Update*, Commonwealth of Australia, Canberra, p. 88.

—— 2022c, *Positioning Australia as a leader in digital economy regulation - Automated Decision Making and AI Regutlation*, Commonwealth of Australia, Canberra.

Presidente, G. and Frey, C.B. 2022, *The GDPR effect: How data privacy regulation shaped firm performance globally*, CEPR, https://cepr.org/voxeu/columns/gdpr-effect-how-data-privacy-regulation-shaped-firm-performance-globally (accessed 16 December 2022).

PwC (PricewaterhouseCoopers) 2017, *Cyber Security: Director responsibilities in a changing legislative environment*, https://www.pwc.com.au/about-us/insights/non-executive-directors/cyber-security-director-responsibilities-in-a-changing-legislative-environment.html (accessed 25 May 2022).

Qu, J., Simes, R. and O'Mahony, J. 2017, 'How do digital technologies drive economic growth?', *Economic Record*, vol. 93, pp. 57–69.

Queensland Health 2016, *Specialist Outpatient Strategy: Improving the patient journey by 2020*, May, State of Queensland, Brisbane.

RACGP (Royal Australian College of General Practitioners) 2022, *General Practice Crisis Summit: White paper*, November, RACGP, East Melbourne, Vic.

RAI (Regional Australia Institute) 2016, *The Economic Contribution of Regions to Australia's Prosperity*, Regional Australia Institute, Canberra.

RDV (Regional Development Victoria) 2021, *Regional Digital Fund*, https://www.rdv.vic.gov.au/grants-and-programs/regional-digital-fund (accessed 8 June 2022).

Reset Australia 2021, *Did we really consent to this? Terms & Conditions and young people's data*, July.

Rinta-Kahila, T., Gillespie, N., Asadi Someh, I. and Indulska, M. 2021, *How to avoid algorithmic decision-making mistakes: lessons from the Robodebt debacle*, https://stories.uq.edu.au/momentum-magazine/robodebt-algorithmic-decision-making-mistakes/index.html (accessed 6 July 2022).

RMIT Online and Deloitte Access Economics 2021, *Ready, Set, Upskill: Effective Training for the Jobs of Tomorrow*.

RMIT (Royal Melbourne Institute of Technology) 2022, *Courses & degrees*, https://online.rmit.edu.au/courses?category=short (accessed 17 May 2022).

Robert, S. 2021, *Public consultation opened on Australia's Digital Identity Legislation*, Ministers' Media Centre, https://ministers.dese.gov.au/robert/public-consultation-opened-australias-digital-identity-legislation (accessed 24 November 2022).

—— and Hume, J. 2021, *6 million Australians using Digital Identity to access online services*, Ministers' Media Centre, https://ministers.dese.gov.au/robert/6-million-australians-using-digital-identity-access-online-services (accessed 24 November 2022).

RTIR Committee (Regional Telecommunications Independent Review Committee) 2021, *2021 Regional Telecommunications Review: A step change in demand*, Australian Government.

Sadler, D. 2022, 'Reworked data-sharing legislation returns to Parliament with Labor's support', *InnovationAus*.

Scottish Government 2018, *Safe, secure and prosperous: A cyber resilience strategy for Scotland — Private sector action plan 2018-20*, June, Scottish Government, Edinburgh.

Shah, R. 2020, *Working smarter, not harder*, Australian Strategic Policy Institute.

—— 2022, *The future of digital identity in Australia*, APSI: The Strategist, https://www.aspistrategist.org.au/the-future-of-digital-identity-in-australia/ (accessed 24 November 2022).

Shergold, P., Broadbent, J., Marshall, I. and Varghese, P. 2022, *Fault lines: An independent review into Australia's response to COVID-19*, 20 October, https://independentcovidreview.com/wp-content/uploads/2022/10/FAULT-LINES-1.pdf (accessed 2 December 2022).

Sier, J. 2022, 'Logan uses government data to transform kindergarten', *Australian Financial Review*, 3 July.

Smedes, M., Nguyen, T. and Tenburren, B. 2022, 'Valuing data as an asset, implications for economic measurement', presented at Economic Implications of the Digital Economy Conference, Sydney, NSW, Australian Bureau of Statistics, March.

Smith, P. 2022, 'Directors and industry at risk from "knee-jerk" tech policies', *Australian Financial Review*, 14 March.

Smith, Z.M., Lostri, E. and Lewis, J. 2020, *The Hidden Costs of Cybercrime*, 9 December, Center for Strategic and International Studies (CSIS) & McAfee, San Jose, CA.

Statistics Canada 2019, *The value of data in Canada: Experimental estimates*, https://www150.statcan.gc.ca/n1/pub/13-605-x/2019001/article/00009-eng.htm (accessed 2 June 2022).

TCA (Technology Council of Australia) 2021a, *Australia has a rich resource in its people. Further cultivating a bright, engaged workforce will deepen opportunities for Australia to be a leading digital economy.*, https://techcouncil.com.au/policy/priorities/talent/ (accessed 18 May 2022).

—— 2021b, *Roadmap to Deliver One Million Tech Jobs*, October.

—— 2022, *Australia's Tech Jobs Opportunity – Cracking the Code to Australia's Best Jobs*, March.

TechnologyOne 2019, *Saas vs On-premise*.

TGA (Therapeutic Goods Administration) 2017, *International agreements and arrangements for GMP clearance*, https://www.tga.gov.au/international-agreements-and-arrangements-gmp-clearance (accessed 27 June 2022).

The White House 2021, *Executive Order on Improving the Nation's Cybersecurity*, 12 May.

Thomas, J., Barraket, J., Parkinson, S., Wilson, C., Holcombe-James, I., Brydon, A. and Kennedy, J. 2021, *Australian Digital Inclusion Index: 2021*, RMIT and Swinburne University of Technology, and Telstra, Melbourne.

Tonkin, C. 2021, *Robodebt was an AI ethics disaster*, https://ia.acs.org.au/article/2021/robodebt-was-an-ai-ethics-disaster.html (accessed 6 July 2022).

Treasury 2021a, *Consumer Data Right in the energy sector: Proposals for further consultation August 2021*, August.

—— 2021b, *Government Response to the Inquiry into Future Directions for the Consumer Data Right*, December.

—— 2022a, *Consumer Data Right - Exposure draft legislation to enable action initiation*, https://treasury.gov.au/consultation/c2022-317468 (accessed 16 December 2022).

—— 2022b, *Consumer Data Right Strategic Assessment: Outcomes*, January.

—— 2022c, *Statutory Review of the Consumer Data Right*, Australian Government, Canberra.

UC (University of California Presidential Working Group on AI) 2021, *Responsible Artificial Intelligence*, October.

UN DESA (United Nations Department of Economic and Social Affairs) 2020, *E-Government Survey 2020: Digital Government in the Decade of Action for Sustainable Development*, United Nations, New York.

UNESCO (United Nations Educational, Scientific and Cultural Organization) 2021, *UIS.Stat - Education - Other policy relevant indicators - Distribution of tertiary graduates by field of study*, http://data.uis.unesco.org/ (accessed 31 May 2022).

United States' Congress 2019, *H.R.2231 - Algorithmic Accountability Act of 2019*.

VHA (Vodafone Hutchison Australia) 2016, *Telecommunications Universal Service Obligation Issues Paper*, July.

Vopson, M.M. 2020, 'The information catastrophe', *AIP Advances*, vol. 10, no. 8, p. 085014.

Vu, K. 2013, 'Information and Communication Technology (ICT) and Singapore's Economic Growth', *Information Economics and Policy*, vol. 25, pp. 284–300.

Weaver, J. and O'Connor, S. 2022, *Tending the Tech-Ecosystem: Who should be the tech-regulator(s)?*, ANU Tech Policy Design Centre, Canberra, ACT.

WEF (World Economic Forum) 2020a, *A Roadmap for Cross-Border Data Flows: Future-Proofing Readiness and Cooperation in the New Data Economy*, June.

—— 2020b, *The Future of Jobs Report 2020*, October.

—— 2022, *Global Cybersecurity Outlook 2022*, January.

Westendorf, T. 2022, *Artificial intelligence and policing in Australia*, April, Australian Strategic Policy Institute.

Williams, S. 2022, 'Greater balance needed in AU Critical Infrastructure Bill', *IT Brief*.

World Bank 2021a, *Global Data Regulation Diagnostic Survey Dataset 2021*, https://microdata.worldbank.org/index.php/catalog/3866 (accessed 13 May 2022).

—— 2021b, *World Development Report 2021: Data for better lives*, World Bank, Washington, DC.

Xero 2021a, *One step: Behavioural barriers to technology adoption amongst small businesses – and how to overcome them*, November.

—— 2021b, *Xero ecosystem survey: Summary of findings*, September.

Zhang, D., Mishra, S., Brynjolfsson, E., Etchemendy, J., Ganguli, D., Grosz, B., Lyons, T., Manyika, J., Niebles, J.C., Sellitto, M., and others 2021, *The AI Index 2021 Annual Report*, March, AI Index Steering Committee, Human-Centered AI Institute, Stanford University, Stanford, CA.