



Harnessing data and digital technology

Interim report



This is an interim report prepared for further public consultation and input. The PC will finalise its report after these processes have taken place.

August 2025



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 (PC) 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 PC'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.

For more information, visit the PC's website: www.pc.gov.au

© Commonwealth of Australia 2025



With the exception of the Commonwealth Coat of Arms and content supplied by third parties, this copyright work is licensed under a Creative Commons Attribution 4.0 International licence. In essence, you are free to copy, communicate and adapt the work, as long as you attribute the work to the PC (but not in any way that suggests the PC endorses you or your use) and abide by the other licence terms. The licence can be viewed at: creativecommons.org/licenses/by/4.0.

The terms under which the Coat of Arms can be used are detailed at: www.pmc.gov.au/government/commonwealth-coat-arms.

Wherever a third party holds copyright in this material the copyright remains with that party. Their permission may be required to use the material, please contact them directly.

An appropriate reference for this publication is:
Productivity Commission 2025, *Harnessing data and digital technology*, Interim report, Canberra, August

Publication enquiries:
Phone 03 9653 2244 | Email publications@pc.gov.au

Opportunity for comment

The Productivity Commission thanks all participants for their contribution to this Inquiry and now seeks additional input for the final report.

You are invited to examine this interim report and comment on it by written submission to the PC, preferably in electronic format, by 15 September 2025.

Further information on how to provide a submission is included on the website:

www.pc.gov.au/inquiries/current/data-digital

The PC will prepare the final report after further submissions have been received, and it will hold further discussions with participants.

Commissioners

Stephen King Commissioner

Julie Abramson Commissioner

Terms of reference

I, Jim Chalmers, pursuant to Parts 2 and 3 of the *Productivity Commission Act 1998*, hereby request that the Productivity Commission (“the Commission”) undertake five inquiries to identify priority reforms under each of the five pillars of the Government’s productivity growth agenda and formulate actionable recommendations to assist governments to make meaningful and measurable productivity-enhancing reforms.

Background

Productivity growth is the key driver of real wage growth and rising living standards over the long term but has been slowing around the world since the mid-2000s. Australia’s productivity growth in the decade to 2020 was the slowest in 60 years.

Several long-standing factors have contributed to the productivity slowdown, including reduced dynamism and competitive pressures, and slower diffusion of technological innovations. Australia also faces new and emerging opportunities and challenges from the changing nature of our economy, including population ageing, rising demand for care and support services, technological and digital transformation, climate change and the net zero transformation, and geopolitical risk and fragmentation. How well we position for and respond to these changes will have a significant impact on our future productivity.

In 2023, the Government set out five pillars for a broad and ambitious productivity growth agenda, and it has already progressed significant reforms under each pillar of this agenda. It is now tasking the Productivity Commission to identify the highest priority reform areas under each of the five pillars which have potential to materially boost Australia’s productivity growth going forward, and the measurable impact of these reforms where possible.

Scope of the inquiries

The Commission will conduct five inquiries to identify and report on priority reforms in each of the areas under the Government’s five pillar productivity growth agenda. Specifically, these are priority reforms which enhance productivity through:

- a. Creating a more dynamic and resilient economy
- b. Building a skilled and adaptable workforce
- c. Harnessing data and digital technology
- d. Delivering quality care more efficiently
- e. Investing in cheaper, cleaner energy and the net zero transformation

The Commission should have regard to other current and recent reviews of relevance to Australia’s productivity performance including the Treasury Competition Taskforce, the National Competition Review and the House Economics Committee inquiry into promoting economic dynamism, competition and business formation; and the objectives and priorities outlined in the Intergenerational Report, the Employment White Paper, the Economic and Fiscal Strategy, the Measuring What Matters statement, and the Government’s legislated emissions reduction targets.

The inquiries should identify prospective areas for reform in the coming years, recognising the findings of recent reviews and taking into account Government reforms and reform directions.

Process

The Commission should engage widely and undertake appropriate public consultation processes, including inviting public submissions. The Commission should engage actively with Commonwealth, and state and territory governments.

The Commission's advice should clearly convey the importance of the reform opportunities identified, including quantitative analysis of the measurable benefits of the priority reforms where possible. This could include the long-run economic impacts on GDP and other measures of economic progress and national prosperity, the benefits accruing to Australian households including distributional impacts where possible, or other outcomes such as improved quality of services or living standards. This analysis should be presented in a way which acknowledges and manages the measurement challenges impacting some important reform areas.

The Commission should publish an interim report for each inquiry in the middle of 2025 that includes preliminary actionable recommendations for productivity-enhancing reforms under the relevant pillar. The final reports for these inquiries should include advice on reform implementation, including implementation feasibility and risks, and be provided to Government within 12 months of receipt of this request.

The Hon Jim Chalmers MP
Treasurer

[Received 13 December 2024]

Disclosure of interests

The *Productivity Commission Act 1998* specifies that where Commissioners have or acquire interests, pecuniary or otherwise, that could conflict with the proper performance of their functions they must disclose those interests.

- Commissioner Stephen King advised that he is currently leading a statutory review of the *Data Availability and Transparency Act 2022* (Cth).
- Commissioner Stephen King advised that he is employed part-time as a Professor of Practice (Economics) at Monash University and is associated with the Digital Lab in the Business School at Monash University.

Acknowledgments

The Commissioners express their appreciation to the staff who worked on the interim report – Assistant Commissioner Jared Dent, who leads the Inquiry, and other team members including Bonnie Nguyen, Shaun McMahon, Colin Burns, Michael Youren, Louisa Borland, Victoria Nguyen, Sean Sutton and Celene Wong. Our thanks are also extended to Yvette Goss and Tracey Horsfall for administrative and project support.

The results of this study are based, in part, on data supplied to the ABS under the *Taxation Administration Act 1953*, *A New Tax System (Australian Business Number) Act 1999*, *Australian Border Force Act 2015*, *Social Security (Administration) Act 1999*, *A New Tax System (Family Assistance) (Administration) Act 1999*, *Paid Parental Leave Act 2010* and/or the *Student Assistance Act 1973*. Such data may only be used for the purpose of administering the *Census and Statistics Act 1905* or performance of functions of the ABS as set out in section 6 of the *Australian Bureau of Statistics Act 1975*. No individual information collected under the *Census and Statistics Act 1905* is provided back to custodians for administrative or regulatory purposes. Any discussion of data limitations or weaknesses is in the context of using the data for statistical purposes and is not related to the ability of the data to support the Australian Taxation Office, Australian Business Register, Department of Social Services and/or Department of Home Affairs' core operational requirements.

Legislative requirements to ensure privacy and secrecy of these data have been followed. For access to PLIDA and/or BLADE data under Section 16A of the ABS Act 1975 or enabled by section 15 of the *Census and Statistics (Information Release and Access) Determination 2018*, source data are de-identified and so data about specific individuals has not been viewed in conducting this analysis. In accordance with the *Census and Statistics Act 1905*, results have been treated where necessary to ensure that they are not likely to enable identification of a particular person or organisation.

Contents

Opportunity for comment	iii
Terms of reference	iv
Executive summary	1
Draft recommendations	2
About this inquiry	5
The data and digital technology opportunity	5
Our package of reforms	6
1. Enable AI's productivity potential	9
The PC's blueprint for AI regulation	17
Case study: copyright law in the age of AI	24
2. New pathways to expand data access	29
Data about you should be available for you to use	30
New regulatory pathways to expand data access	37
What might new access pathways look like?	43
3. Supporting safe data access and use through outcomes-based privacy regulation	51
The Privacy Act in a changing data landscape	53
Renewing the focus on privacy outcomes	58
Proposed reforms risk entrenching existing problems	64
4. Enhance reporting efficiency, transparency and accuracy through digital financial reporting	69
We are forgoing the benefits of digital financial reporting	70
Digital financial reporting should be the default	76
The PC is seeking feedback on implementation issues	82
Appendices	86
A. Public consultation	87
B. Modelling the benefits of data and digital reforms	95
B.1 Summary	95

B.2	Improved use of data	96
B.3	Reducing privacy compliance burdens	98
B.4	Estimating the productivity effects of AI	100
Abbreviations		106
References		108

Executive summary

Data and digital technologies are the modern engines of economic growth. Emerging technologies like artificial intelligence (AI), which can extract useful insights from massive datasets in a fraction of a second, could transform the global economy and speed up productivity growth.

Australia needs to harness the consumer and productivity benefits of data and digital technology while managing and mitigating the downside risks. There is a role for government in setting the rules of the game to foster innovation and ensure that Australians reap the benefits of the data and digital opportunity.

The economic potential of AI is clear, and we are still in the early stages of its development and adoption. Early studies provide a broad range of estimates for the impact of AI on productivity. The Productivity Commission considers that multifactor productivity gains above 2.3% are likely over the next decade, though there is considerable uncertainty. This would translate into about 4.3% labour productivity growth over the same period. But poorly designed regulation could stifle the adoption and development of AI and limit its benefits. Australian governments should take an outcomes-based approach to AI regulation – one that uses our existing laws and regulatory structures to minimise harms and introduces technology-specific regulations as a last resort.

Data access and use can fuel productivity growth: insights from data can help reduce costs, increase the quality of products and services and lead to the creation of entirely new products. But some requirements in the Privacy Act, the main piece of legislation for protecting privacy, are constraining innovation without providing meaningful protection to individuals. For example, complying with the controls and processes baked into the Act can make consent and notification a ‘tick box’ exercise – where businesses comply with the letter of the law but not the spirit of it. The Australian Government should amend the Privacy Act to introduce an alternative compliance pathway that enables firms to fulfil their privacy obligations by meeting outcomes-based criteria.

Data about individuals and businesses underpins growth and value in the digital economy. But often those same individuals and businesses cannot easily access and use this data themselves. Under the right conditions, giving people and businesses better access to data that relates to them can stimulate competition and allow businesses to develop innovative products and services. A mature data-sharing regime could add up to \$10 billion to Australia’s annual economic output.

Experience shows that we need a flexible approach to facilitating data access across the economy, where obligations placed on data holders and the level of government involvement can match the needs and digital maturity of different sectors. New lower-cost and flexible regulatory pathways would help to guide expanded data access throughout the digital economy, focusing first on sectors where the gains can be significant and relatively easy to achieve.

Financial reports provide essential information about a company’s financial performance, ensuring transparency and accountability while informing the decisions of investors, businesses and regulators. Government can further spark productivity by making digital financial reporting the default – that is, mandatory lodgement of financial reports in machine-readable form. At the same time, the Australian Government should remove the outdated requirement that financial reports be submitted in hard copy or PDF format. This change would increase the efficiency and accuracy with which information is extracted and analysed.

Draft recommendations

Artificial intelligence



Draft recommendation 1.1

Productivity growth from AI will be built on existing legal foundations. Gap analyses of current rules need to be expanded and completed.

Australian governments play a key role in promoting investment in digital technology, including AI, by providing a stable regulatory environment. Any regulatory responses to potential harms from using AI must be proportionate, risk-based, outcomes-based and technology-neutral where possible.

The Australian Government should continue, complete, publish and act on ongoing reviews into the potential gaps in the regulatory framework posed by AI as soon as possible.

Where relevant gap analyses have not begun, they should begin immediately.

All reviews of the regulatory gaps posed by AI should consider:

- the uses of AI
- the additional risk of harm posed by AI (compared to the status quo) in a specific use-case
- whether existing regulatory frameworks cover these risks potentially with improved guidance and enforcement; and if not how to modify existing regulatory frameworks to mitigate the additional risks.



Draft recommendation 1.2

AI-specific regulation should be a last resort

AI-specific regulations should only be considered as a last resort for the use cases of AI that meet two criteria. These are:

- where existing regulatory frameworks cannot be sufficiently adapted to handle the issue
- where technology-neutral regulations are not feasible.



Draft recommendation 1.3

Pause steps to implement mandatory guardrails for high-risk AI

The Australian Government should only apply the proposed ‘mandatory guardrails for high-risk AI’ in circumstances that lead to harms that cannot be mitigated by existing regulatory frameworks and where new technology-neutral regulation is not possible. Until the reviews of the gaps posed by AI to existing regulatory structures are completed, steps to mandate the guardrails should be paused.

Data access



Draft recommendation 2.1

Establish lower-cost and more flexible regulatory pathways to expand basic data access for individuals and businesses

The Australian Government should support new pathways to allow individuals and businesses to access and share data that relates to them. These regulatory pathways will differ by sector recognising that the benefits (and the implementation costs) from data access and sharing are different by sector. This could include approaches such as:

- **industry-led data access codes** that support basic use cases by enabling consumers to export relatively non-sensitive data on a periodic (snapshot) basis
- **standardised data transfers** with government helping to formalise minimum technical standards to support use cases requiring high-frequency data transfers and interoperability.

These pathways should be developed alongside efforts that are already underway to improve the Consumer Data Right (which will continue to provide for use cases that warrant its additional safeguards and technical infrastructure) and the My Health Record system.

The new pathways should begin in sectors where better data access could generate large benefits for relatively low cost; and there is clear value to consumers. Potential examples include:

- enabling farmers to combine real-time data feeds from their machinery and equipment to optimise their operations and easily switch between different manufacturers
- giving tenants on-demand access to their rental ledgers which they can share to prove on-time payments to new landlords or lenders
- allowing retail loyalty card holders to export an itemised copy of their purchase history to budgeting and price comparison tools that can analyse spending and suggest cheaper alternatives.

The scope of the data access pathways should expand over time based on industry and consumer consultation, where new technology, overseas experience or domestic developments show that there are clear net benefits to Australia.

Privacy regulation



Draft recommendation 3.1 An alternative compliance pathway for privacy

The Australian Government should amend the *Privacy Act 1988* (Cth) to provide an alternative compliance pathway that enables regulated entities to fulfil their privacy obligations by meeting criteria that are targeted at outcomes, rather than controls-based rules.



Draft recommendation 3.2 Do not implement a right to erasure

The Australian Government should not amend the *Privacy Act 1988* (Cth) to introduce a 'right to erasure', as this would impose a high compliance burden on regulated entities, with uncertain privacy benefits for individuals.

Digital financial reporting



Draft recommendation 4.1 Make digital financial reporting the default

The Australian Government should make the necessary amendments to the *Corporations Act 2001* (Cth) and the Corporations Regulations 2001 (Cth) to make digital financial reporting mandatory for disclosing entities. The requirement for financial reports to be submitted in hard copy or PDF format should also be removed for those entities.

About this inquiry

The data and digital technology opportunity

The global economy has been transformed over the past 50 years by advancements in information and communication technology. And this transformation is continuing. Technologies relating to data and digital services – such as emerging ones like artificial intelligence (AI), which can analyse and extract useful insights from massive datasets in a fraction of a second – are the modern engines of economic growth.

New digital technologies – like they have in the past – can create benefits across the entire economy, including speeding up lacklustre productivity growth. The development of information communication technologies contributed up to 0.3 percentage points to Australia's annual economic growth in the late 1990s (PC 2004, p. 7). Similarly, internet and mobile phone adoption increased Australian GDP per capita by about 3% between 2004 and 2014 (Qu et al. 2017, pp. 66–67). AI, and related digital innovations, could offer equivalent or bigger productivity gains. Early estimates suggest AI will increase multifactor productivity by 0.5% to 13% over the next decade. After examining the assumptions underpinning these studies, the Productivity Commission considers that multifactor productivity gains above 2.3% are likely (though there is considerable uncertainty about the precise magnitude). This would translate into about 4.3% labour productivity growth over the next decade (see appendix B for details).

Better data access and use regimes that reduce frictions between data holders, users, and subjects – consumers and businesses – can enable the development of new digital technologies. Less friction can also spur productivity growth more broadly: insights from data can help reduce the cost of doing business, increase the quality of products and services for consumers and lead to the creation of entirely new products (PC 2023b, p. 1). In 2019, the OECD found that data sharing 'generate[d] social and economic benefits worth between 0.1% and 1.5% of gross domestic product (GDP) in the case of public-sector data, and between 1% and 2.5% of GDP (in a few studies up to 4% of GDP) when also including private-sector data' (2019, p. 11).

Australians are already generating and sharing vast amounts of data about themselves both directly (such as by uploading content to social media), and as a byproduct of other activities (such as through online shopping). They are also embracing new digital technologies. As of March 2023 an estimated 68% of Australian businesses had already adopted AI technologies, and a further 23% reported that they were planning to do so in the next 12 months (CSIRO 2023, p. 16; Export Finance Australia 2023). While businesses can access and use this trove of data to create and offer better, more personalised services, that same option is not always available for consumers who might also want to use data to find goods and services that are a better fit for them. The relative ease with which massive amounts of data can be created, gathered, stored and traded also creates issues of privacy and trust.

Australia needs a way forward that enables the consumer and productivity benefits from data and digital technology to be harnessed, and the downside risks mitigated. There is a role for government in setting the rules of the game, but without unduly curtailing the benefits of data and digital technologies and stifling innovation.

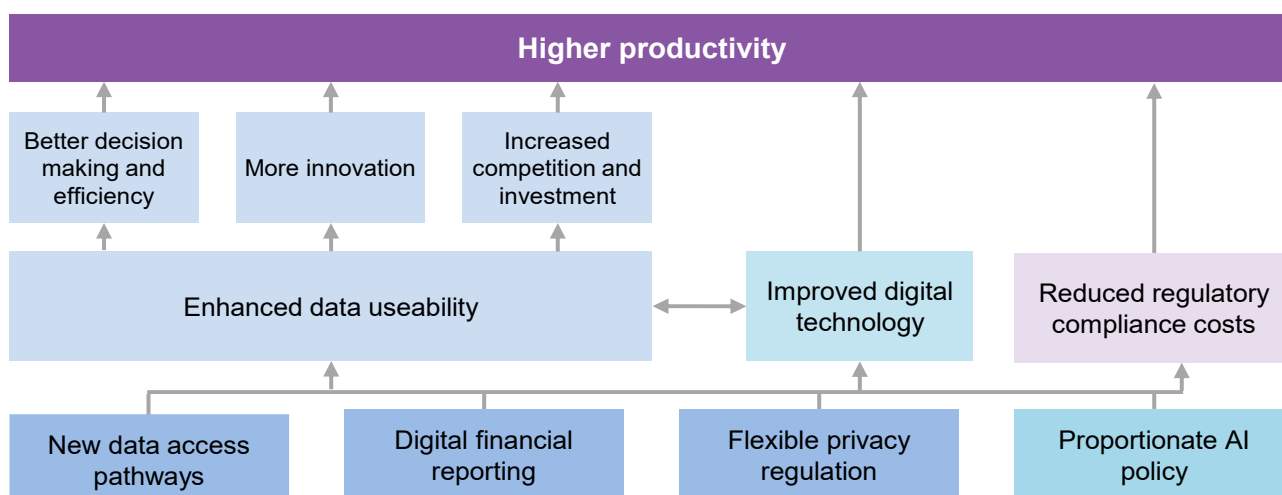
Our package of reforms

In January 2025, we asked for ideas about improving productivity through data and digital technologies. We received a wide range of ideas from government, industry and the community. We also looked at what work is already being progressed elsewhere in government – such as the review of the Data Availability and Transparency Act, work to progress the Data and Digital Government Strategy, initiatives to expand the Digital ID system, and the recent *2024 Regional Telecommunications Review*.

On this basis, we identified reform options in four policy areas to boost overall productivity (figure 1), taking account of the unique nature of data and digital technology (box 1).

- **AI technology** is already being used to enhance productivity across Australia. Some economists predict that AI could create productivity growth similar to previous groundbreaking technologies – like the steam engines that powered the Industrial Revolution in the 1800s and electricity that powered manufacturing in the 1900s. Chapter 1 sets out a blueprint for identifying the right regulatory settings that will enable Australia to make the most of this opportunity.
- Data about individuals and businesses underpins growth and value in the digital economy. Our **data access** reform is about enabling Australians to harness these benefits (chapter 2). With better access to data that relates to them, people and businesses could save time and money by linking up the products and services they use or more easily switching to new providers. They could also access data-driven services to better manage their health and finances or improve their business operations.
- The benefits of data access and use can only be realised if they are underpinned by trust that data is being handled safely and securely. One way that governments seek to achieve this is through **privacy regulation**. The policy challenge is that, if implemented poorly, privacy regulation can harm productivity – whether because compliance unduly burdens businesses or because it fails to protect the privacy interests of individuals, thereby undermining trust. This issue is explored in chapter 3.
- The adoption of **digital financial reporting** would increase the efficiency and accuracy with which financial information can be extracted and analysed. It would enable more effective decision-making by investors (including the many Australians who hold shares directly or through superannuation funds), businesses and regulators, while promoting transparency and accountability. We outline how these benefits can be realised in chapter 4.

Figure 1 – Four reform areas to support productivity growth



The reforms in this report will create an enabling environment that fosters data access and use so that consumers, businesses and governments alike can harness the benefits of data and digital technology. They

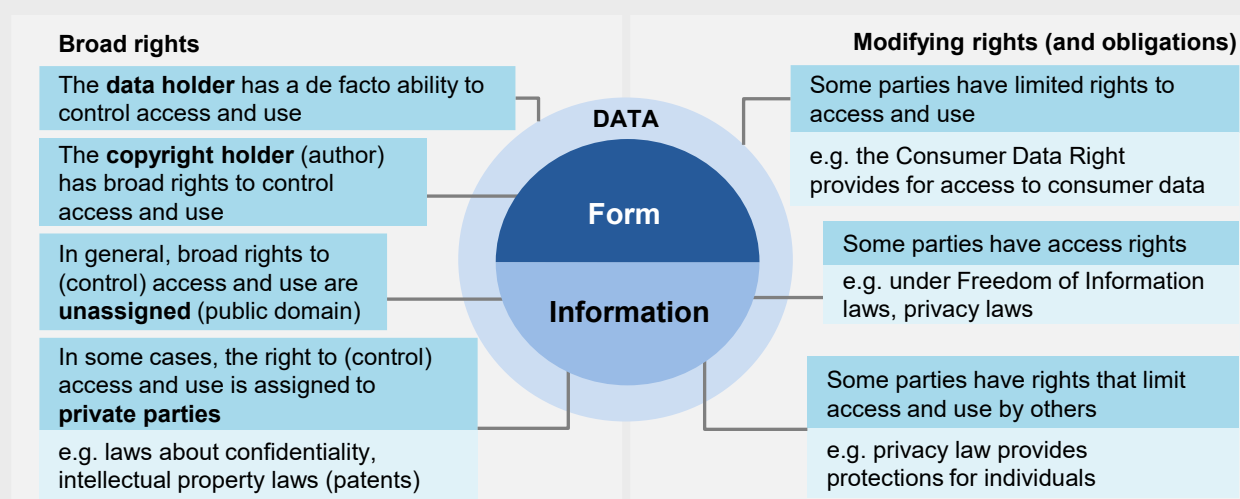
are also about building a system that includes the right regulatory safeguards and protections, so that Australian consumers and businesses can participate with confidence.

Box 1 – What makes data unique?

There are overlapping interests in data

Data is the encoding of information into any form, including text, audio and visual material in analogue or digital formats. Data is not exclusively owned by any single party; instead, the law recognises overlapping interests (depicted in the figure below). While data holders have broad, de facto control over data, this may be subject to other legal interests or obligations. This includes rights in relation to the component parts of the data, such as:

- the underlying information captured by the data – which is generally considered to be in the public domain but can be subject to access regimes and privacy laws
- the form in which data is expressed – which may be subject to, for example, copyright claims.



One key policy issue is how these different interests should be traded off against each other when they come into conflict – and laws, regulation and policy on this matter are constantly evolving.

Data access and use is non-rivalrous

Data is distinct from other goods in that it is often non-rivalrous, meaning multiple parties can access and use the same data at the same time without depleting its value to other users. This means data has high potential value as an economic good because, once the (typically low) cost of encoding it is incurred, it can be shared widely and stored with almost no additional production cost. This implies that, once created, economic welfare is maximised by the widest possible use of data, subject to any negative externalities (discussed below). In other words, data could be **under shared** relative to the optimal level.

Data access and use can create risks

Data access and use can also be associated with negative externalities. For example, when data includes personal information, an individual may be made worse off if it is widely shared as this undermines their privacy. This could mean that, in the absence of regulation to limit or mitigate those negative externalities, data can also be **over shared** relative to the optimal level.

1. Enable AI's productivity potential

Summary

- ✳ **Artificial Intelligence (AI) could underpin a new wave of productivity growth.** Early estimates suggest AI will increase multifactor productivity by 0.5% to 13% over the next decade. The Productivity Commission considers that productivity gains above 2.3% are likely, although there is considerable uncertainty. This would translate to about 4.3% labour productivity growth over the next decade.
 - Examples of Australian uses of AI happening right now include fraud detection and warnings by banks, robotic sorting in agriculture, and teaching tools at schools and universities.
- ✳ **As with any new technology, AI can raise risks. Getting regulatory settings right will help keep Australian consumers safe and give businesses the certainty they need to use, invest and develop AI technologies.**
 - Poorly designed regulations could stifle AI investment without improving outcomes.
- ✳ **Existing regulations are the starting point. Governments are conducting gap analyses to assess whether existing regulations sufficiently address AI-related risks. Regulatory changes should only be considered if clear gaps are identified.**
- ✳ **AI-specific regulations should only be considered as a last resort when it is not feasible to adapt existing regulatory frameworks or introduce technology-neutral regulations.**
- ✳ **An example of where governments can act to bring regulatory clarity and certainty is in copyright settings. The PC is seeking feedback about whether reforms are needed to better facilitate the use of copyrighted materials, in the context of training AI models.**

Artificial intelligence is part of the solution to anaemic productivity growth

Artificial Intelligence (AI) could underpin a new wave of productivity growth in Australia and around the world (box 1.1).

AI adoption is in its early stages, but people are already embracing this technology and realising real efficiency and productivity gains. Law firms use 'large language models' for evidence review and preliminary drafting (Snowden 2025b, 2025a) and teachers are using AI models as an education tool (Kowal 2025). AI

tools are helping logistics companies improve their last mile delivery by better responding to real time changes in customer demand, internal priorities and fleet availability (DHL 2024). The public is rapidly adopting AI tools as well. A popular AI Assistant, ChatGPT, had over 100 million users two months after its release and about 500 million people currently use it every week (Milmo 2023; OpenAI 2025a, p. 6).

As AI continues to develop and its uses become clearer, the potential upside productivity benefits, including from as yet undiscovered AI applications and improvements in the underlying models themselves, could be significant.

Box 1.1 – How large is the productivity dividend from AI?

AI will likely raise productivity, but there is ongoing debate about the magnitude of this effect. Studies suggest AI could increase multifactor productivity between 0.5% to 13% over the next decade (0.05 to 1.3 percentage points annually). After examining the assumptions underlying these studies, the PC considers that multifactor productivity gains above 2.3% are likely over the next decade (0.23 percentage points annually). As a back of the envelope, this would imply labour productivity growth of about 4.3%, which at current levels of population, working hours and employment would imply about an extra \$116 billion of GDP over the next decade. That said, there is considerable uncertainty about the precise magnitude of the productivity effect.

In the long term, AI productivity gains could be well above 2.3%. AI may accelerate the pace of scientific progress, contributing to permanently higher economic growth (Aghion and Bunel 2024, p. 12). And as AI capability improves, AI may also play an increasingly large role and could be leveraged for completely new applications (Filippucci et al. 2024, p. 17).

However, some productivity benefits may go unmeasured. AI is likely to lead to completely new products and improve the quality of existing products. But the contribution of new products and quality improvements tend to be underestimated in official statistics (Feldstein 2017), especially when they are free. For instance, properly accounting for free digital content may mean annual US GDP growth was 0.11 percentage points higher between 2005–2015 (Nakamura et al. 2017). Additionally, investments required for AI adoption may be challenging to measure, potentially delaying gains in measured productivity improvement (Brynjolfsson et al. 2021).

Governments have a key role in making the most of the AI opportunity

The Productivity Commission (2024d, p. 10) considers that the Australian Government has a number of policy responsibilities that will be important in making the most of the AI opportunity.

- *Using regulation sensibly to build community trust and business confidence* – consistent and reliable regulation can help promote trust in AI technology, which in turn creates an environment in which business is willing to invest in, develop, and adopt AI.
- *Acting as an exemplar in the use of AI* – governments are some of the largest employers of professionals in the country and so will likely be a large user of AI technologies. This means governments' internal policies towards AI can have a significant impact on the uptake of this technology.
- *Building foundational capabilities to support AI uptake* – governments play a major role in regulating and funding education and training in Australia. As a result, governments will be key players in determining whether these systems are able to provide the digital literacy necessary for effective AI use.

- *Investing in digital infrastructure* – as many AI models will not be hosted locally, high-speed internet is a prerequisite to fully utilising AI. Governments have a key role to play in providing the digital infrastructure necessary for high-speed internet.

This reform proposal focuses on government regulation. This focus was chosen for a variety of reasons, including: the lack of international consensus on the best way to regulate AI, calls from industry for more certainty on the ways AI risk and opportunities will be handled by regulators, the overlap of some of these key areas with other inquiries running concurrently with this one (such as skills and education) and concerning proposals for the regulation of AI in Australia. However, all these levers will be important in grasping the AI opportunity and Australian governments should be reflecting on their performance in each of these areas.

For the purposes of this inquiry, AI is defined as any systems that perform tasks usually requiring human intelligence (box 1.2).

Box 1.2 – What is artificial intelligence?

AI refers to machine systems that perform tasks typically requiring human intelligence, such as learning, reasoning, and decision-making (Digital NSW 2025). Unlike traditional algorithms – where humans specify how to perform a task – AI models can infer how to generate outputs from inputs, often with minimal human oversight.^a

AI is commonly categorized by function:

- Generative AI – responds to prompts to create text, images, video, or other data.^b
- Agentic AI – makes autonomous decisions and performs tasks independently, often using Generative AI.

AI models are also classified by scope:

- Narrow AI (or weak AI) – includes current systems like chatbots, which are trained for specific tasks.
- Artificial General Intelligence (or AGI) – is a hypothetical form of AI capable of performing any intellectual task a human can (Digital NSW 2025). Some refer to generative AI models like ChatGPT, Claude and Grok as ‘general purpose AI’ (GPAI), which should not be confused with AGI.

a. The ability of some artificial intelligence models to find patterns in data and use this to make predictions or create new media is referred to as ‘machine learning’ (Stryker and Kavlakoglu 2024). **b.** Generative AI models use the same machine learning methods employed by other types of AI models (typically trained on a massive dataset with millions of observations and parameters). What distinguishes Generative AI is that rather than just producing numerical output, it can create new text, audio or video content. This is accomplished by converting textual, audio or video information into numerals (‘tokenisation’) that a computer can understand. The model then produces an output in numerical form that is then converted into text, audio or video (Salvator 2025). Models with the ability to interpret different types of inputs are referred to as ‘multimodal’, and some of these models can produce one type of output when asked, say an image, but when asked a different prompt can produce a different type of output, for example text (Stryker 2024).

How AI could affect productivity

Automation, machines performing tasks that were previously performed by humans, has driven much of the productivity growth we have seen since the Industrial Revolution (Aghion et al. 2017, pp. 3–4; Autor et al. 2003, p. 1284). Automation can increase incomes, leisure time, and, living standards when machines perform tasks faster or better than human labour. For example, replacing ploughs with tractors leads to bigger harvests with less work.

As technology advances, human workers often shift to tasks that are harder to automate, and new tasks are also created. This process is known as *augmentation*, where machines enhance rather than replace human roles. Hand calculators, for example, automated and greatly increased the speed and accuracy of the calculations required to solve complex problems (like launching rockets) but also allowed skilled labour to be freed up for other tasks that add more value (like designing better rockets).

AI continues the trend of automation and augmentation. But, whereas tools like the tractor affected manual tasks, AI, like the introduction of computers, has the potential to automate cognitive tasks.

Unlike computerisation, which mostly automated *routine* cognitive tasks like data entry or typewriting (Autor et al. 2003), AI appears to be replacing *non-routine* cognitive tasks (Autor 2024, p. 7). This includes things like enabling robots to fetch goods in an Amazon warehouse (partially enabled by having a sense of touch) (Amazon 2025).¹ But this also includes more creative tasks like composing new text, and audio and visual media as well as creating computer programs from scratch.²

There is also the possibility that AI could affect the pace of scientific progress itself (box 1.3).

Box 1.3 – AI could change the pace of scientific progress

AI has already been applied in medical research, physics and chemistry (Charley 2024; Devlin 2025; ScienceDaily 2024). This could speed up the discovery and development of new technologies, leading to faster economic growth.

To take an example from biology, the AI program AlphaFold uses an algorithm trained on 170,000 previously solved proteins to predict other protein structures, of which millions remain unsolved (Service 2020). Protein prediction is an incredibly complex process. Predicting structures would previously take researchers months or years, but with AlphaFold it now takes minutes (Isaacson 2024). The program greatly increases the ability of scientists to understand diseases and identify possible treatments. Venki Ramakrishnan, winner of the 2009 Nobel Prize in Chemistry, stated that the program has produced results that have ‘occurred decades before many people would have predicted’, and that the program will ‘fundamentally change biological research’ (Deepmind 2020). It is not clear how much AI will affect the pace of scientific research, and even less clear how that will then affect economic growth but these early applications seem highly promising.

AI is already changing Australian workplaces

Inquiry participants told the PC about the many areas where AI is being actively rolled out.

- *Repetitive administration tasks* – many have used AI tools to save time on various administrative tasks such as drafting emails, responding to customer inquiries or scheduling activities (ADHA, qr. 16, pp. 8; Marrickville Legal Centre, qr. 38, p. 3; MFAA, qr. 67, p. 3; Osjavi Rana, qr. 68, p. 3; TCA, qr. 69, p. 4).
- *Education and training* – a variety of AI tools are being used by educators to augment their teaching (The University of Sydney, qr. 21, p. 6; RUN, qr. 22, pp. 3–4; CAG TAFE, qr. 41, p. 3).

¹ In the same way that humans learn to ride a bicycle over time through trial and error – instead of learning the actual physics required – Amazon’s Vulcan robot has learnt by ‘figuring out how different objects behave when touched and steadily building up an understanding of the physical world, just like kids do’ (Amazon 2025). This process can be referred to as ‘non-routine’, as algorithms could not be pre-programmed by humans to dictate Vulcan’s decision making.

² Potential copyright issues raised by the training process for AI models are discussed below.

- *Software and IT systems* – other participants are using AI tools and processes as part of the development of software or for internal cybersecurity purposes (Montu Group Pty Ltd, qr. 35; p 3; Atlassian, qr. 50, p. 6; Microsoft, qr. 52, pp. 4–5; Salesforce, qr. 57, pp. 3–4).

The PC also learned of many other Australian applications of AI. Lyro Robotics has developed an avocado sorting robot that interprets footage to recognise and then sort fruit based on how ripe it is (Field 2025). The Commonwealth Bank of Australia stated that they have seen a 30% drop in customer-reported fraud due to measures like AI powered transaction alerts (2024a). Westpac is piloting a system that detects indications that a customer is being coerced when they call the bank (Westpac 2025). Telstra reduced follow up calls made by customers with service issues by 20% through the use of an AI tool developed in house (Telstra 2024b). Community service providers are also using AI to improve their processes. In far-north Queensland, park rangers are using AI to detect, isolate and catalogue Aboriginal rock art from photos (Richards 2023). Manually cataloguing rock art is otherwise time consuming, with many sites still yet to be discovered. In the Northern Territory, AI analysis of drone footage is being used to identify ghost nets (Ellis 2025). Rangers would otherwise have to visually inspect the coastline themselves.

While AI is being widely applied to a broad range of tasks, the overall macroeconomic effect of AI on the job market – how many jobs will be changed, gained or lost – is highly uncertain (box 1.4). The PC understands that Jobs and Skills Australia plans to release a report examining these effects later in August 2025.

Box 1.4 – How might AI change the mix of roles people work in?

AI, like all previous technological changes, is anticipated to increase the demand for workers in some professions and decrease it for others. Inevitably, this will involve both painful transitions for workers whose roles are made redundant and positive changes from new opportunities. But precisely which occupations will be affected, the amount of job losses, job creations and job changes, and the speed of the transition are all subject to a range of factors.

Part of the complexity in forecasting how AI will affect the structure of the workforce is that just because an occupation has high 'exposure' to AI does not necessarily mean there will be significant job losses in that occupation (Cazzaniga et al. 2024, p. 6). Some tasks performed by AI can be 'complementary' to those performed by humans— meaning that greater use of AI will raise demand for other tasks performed by humans. Even when AI does automate some jobs, other factors can balance out the impact. For instance, AI might make it cheaper to produce goods and services in a certain industry. This could lead to lower prices, which encourages people to buy more of these goods and services. As demand increases, companies may need more of both AI tools and human workers to meet that new demand.

Overall, most forecasts expect AI to result in a net increase in the number of jobs but with there could be a sizeable number of workers that are displaced. For example, a report by the World Economic Forum forecasted, at a global level, a net growth of 2 million jobs due to AI and information processing technologies (including big data, virtual reality and augmented reality), with wider job growth due to AI forecast at 11 million jobs and displacement of 9 million jobs by 2030 (WEF 2025, p. 25). Generally, the World Economic Forum expects that clerical and administrative related roles will have the largest job losses proportionally, while occupations related to IT and digital services will have the greatest gains proportionally (WEF 2025, pp. 19–21). This is consistent with most other early studies, which have projected decreased demand for administrative roles or related skills over the next five years (McKinsey Global Institute 2024, pp. 13–14; OECD 2024a, pp. 35–36).

Box 1.4 – How might AI change the mix of roles people work in?

To the extent significant job displacement does occur the Australian Government may need to consider support for retraining of workers, as has occurred in the past when there have been changes to the way jobs are undertaken. The social safety net of unemployment assistance would also be available.

Jobs and Skills Australia is undertaking fulsome examination of the evidence on how AI could affect the structure of the Australian workforce. This includes looking at the exposure of jobs and different groups of workers to tasks being augmented or automated by AI, and the broader implications for the labour market and skills. The findings and advice are expected to be released in August 2025.

Will AI be the great skill equaliser?

Previous waves of automation have sometimes disproportionately affected workers in roles that required less formal training, resulting in reduced wages or job losses. For instance, the rise of information and communication technologies led to significant job losses in areas such as data entry, bookkeeping, and assembly line work (Autor et al. 2003, pp. 1284–1286). These transitions, while driven by technological progress, had real and lasting effects on individuals and communities.

However, AI presents a different kind of opportunity. It has the potential to enhance productivity not only by automating routine tasks, but also by simplifying complex ones traditionally performed by highly-trained professionals. For example, Generative AI can instantly produce text, audio, and video from a simple written prompt – tasks that previously required specialized skills in media creation (Baily et al. 2023). This shift may help bridge the gap between workers with varying levels of formal training, offering broader access to tools and capabilities that were once limited to a select group. In doing so, AI could support broader access to the gains from technological progress and open new pathways for workers across the skill spectrum.

That said, some economists have noted that even if AI has the effect of automating tasks predominately performed by workers with more formal training, this *may still* have the effect of worsening inequality through offsetting mechanisms. This could include through reducing the labour share of income or through a high degree of complementarity between jobs with high formal training requirements and AI (Acemoglu 2025; Cazzaniga et al. 2024).

Could AI have other benefits at work?

There is also some evidence that greater use of AI could enable marginalised groups to join the workforce. A study by the OECD identified 142 examples of AI powered solutions that could support people with disability in the labour market (2023, p. 8). Examples of tools include a text simplification program to help workers with learning disabilities, and a combined image recognition and text to speech application to help identify currency for low vision people (2023, p. 80).

Mitigating the potential risks of AI

AI, like all previous technological developments, has the potential for misuse, malfunction and unintended consequences leading to harm. Policymakers need to mitigate the risks without forgoing the benefits of AI.

The International AI Safety report groups the potential harms of AI into three categories:

- malicious use – such as fake content, manipulation of public opinion, criminal offenses and biological and chemical attacks
- malfunction – such as reliability issues, bias and loss of control

- systemic risk – such as negative labour market effects, global inequity of R&D capability, market concentration or single points of failure, environmental risks, privacy risks and copyright risks (Bengio 2025, pp. 17–20).

Participants told the PC they were concerned about the potential for AI to cause harm across a wide array of applications for which it could be used.

- Mistakes and hallucinations – concerns AI could make mistakes in high-risk scenarios such as healthcare, financial services, law enforcement or employment (ADHR, qr. 16, p. 9; Salesforce, qr. 57, p. 5; Cancer Council Australia, qr. 64, pp. 7–8).
- Bias and discrimination – AI's outputs reflect its training data. Where training data is biased or marginal groups are not sufficiently represented AI may discriminate (Cancer Council Australia, qr. 11, p. 7; EY Australia, qr. 27, p. 8; MCRI, qr. 34, p. 6; BSA, qr. 73, p. 8).
- Emissions – AI is computationally intensive and there are concerns this will contribute to higher emissions (APDG, qr. 6, p. 5; ATN Universities, qr. 13, p. 3; ASCA, qr. 14, p. 7).
- Threats from harmful actors – concerns that the ability of AI to generate content quickly could increase the ease with which groups could commit harmful acts, such as terrorist attacks (Good Ancestors Policy, qr. 5, p. 4).
- Lack of understanding of AI – concerns that the pace of AI development is outstripping regulators' ability to mitigate associated risks (ADHA, qr. 16, p. 9).

Some participants to the Senate's (2024) Select Committee on Adopting Artificial Intelligence were also concerned about the use of AI by employers. These included concerns about a lack of consultation with workers and the use of AI to monitor employee performance (ACTU 2024; VTHC 2025, p. 5). The PC notes that where enterprise agreements have been made, s. 205 of the *Fair Work Act 2009* (Cth) requires that consultation clauses about major workplace change that is likely to have a significant effect on the employees are included within the agreement, or otherwise a model consultation clause is deemed to be included. Similarly, modern awards – which set out minimum terms and conditions of employment – all have clauses requiring that employers consult with employees regarding major workplace changes that are likely to have significant effects on employees.

Few of AI's risks are wholly new issues

The above examples outline a range of cases where applied AI can *exacerbate* existing risk of harm but does not create *wholly new* risks where none existed before. Indeed, issues like the environmental pressures posed by high energy demands when training and running AI models, or even the potential issue of copyright infringement, are not unique to AI and continue trends seen with previous phases of the information technology revolution.

That said, AI can shift the economic incentives in ways that exacerbate existing problems. The malicious potential of AI stems from its ability to perform antisocial tasks better, much more cheaply and at a greater scale, than humans. This means, for example, that issues like deepfake imagery or manipulation of public opinion by malicious actors – which have existed for a long time – have become much more significant problems because of their lower cost and proliferation.

The regulatory response should focus on mitigating the *additional risk* of these harms occurring, rather than treating them as wholly new problems.

Burdensome regulation risks forfeiting AI's benefits

While governments should aim to mitigate the risk of serious harm, burdensome regulatory requirements can stifle innovation. Indeed, while *some* stifling of innovation is the unavoidable cost of adequate consumer protection, it is important for government to ensure that any regulatory goal is pursued at the lowest cost possible.

There are real world examples of regulations having an unintended chilling effect on innovation. The European Union's (EU) General Data Protection Regulation (GDPR) aims to protect the data rights of individuals, but appears to have stifled innovation and investment (box 3.9).

The mere threat of regulation can hinder innovation if firms believe it may be overly onerous or its direction is highly uncertain. This can lead to firms holding off on investments into emerging technologies out of fear that forthcoming regulations will make the use of these technologies financially unviable.

The PC heard from inquiry participants that this could be the case for AI regulation in Australia.

- The AIIA (qr. 49, p. 6) said that ongoing regulatory uncertainty in finalising legislative processes has been creating a 'wait-and-see' effect, with a 'dampening effect on investment'. It supported the use of existing regulatory frameworks and said that any new laws should only focus on high-risk uses until there is more clarity in AI development. It added that if the government is inclined to enact new laws, 'modern collaborative, agile and principles-based regulation' should be developed in partnership with industry.
- MYOB (qr. 31, pp. 5–6) raised concerns about developing and deploying AI in an environment where AI specific regulation remains unclear. It stated that it would 'value clarity' from the Australian Government regarding the mandatory guardrails legislation. Specifically, it is looking for clarity on the status of the process, what potential timelines may look like, where legal risk and responsibility are likely to sit in the supply chain, and further clarity on definitions of high-risk settings.
- Montu (qr. 35, p. 3) stated that regulatory uncertainty around AI has created 'hesitancy in adoption, as guidelines and liability frameworks remain unclear'. It added that their 'primary concern is the risk of regulatory overreach, where AI use in healthcare is limited or restricted without meaningful consultation with the sector'. Montu suggested appropriate regulation, as an absence of clear regulation 'creates risks of its own', but that overly cautious regulation could slow innovation and reduce access to timely care.

It is difficult to know to what degree these concerns have translated into lower investment flows as there is limited evidence on the relative intensity rates of adoption of, and investment in, AI in Australia compared with overseas peers (box 1.5).

Box 1.5 – Is Australia already lagging in AI take-up?

The evidence on Australia's AI take-up overall shows a mixed picture. While Australians are adopting AI tools, other metrics like AI job adverts imply a less encouraging picture of AI penetration.

However, it is not yet possible to make a definitive comparison between Australia and the rest of the world in terms of AI adoption and investment. The few studies relevant to this issue either focus on the use of very specific tools (such as ChatGPT), look at broader use patterns but only examine a single country at a time (making cross-country comparisons difficult) or examine use metrics with only a weak relationship with actual AI investment and adoption (such as the sentiments of business leaders).

- A World Bank study used country level ChatGPT web traffic data as one measure. It found Australia had the 15th highest level of monthly traffic in March 2024, and that Australia ranked in the top 10 when this was adjusted on a per capita basis (Liu and Wang 2024, p. 24).
- A Deloitte survey of 11,900 individuals, made up of approximately 9,000 employees and 2,900 students in 13 countries in Asia and the Pacific found that use of AI in Australia was lower than the average across Asia Pacific and Southeast Asia, and behind New Zealand (Deloitte 2024b).
- A survey on worldwide AI use conducted by Ipsos for Google included just over 21,000 adults in 21 countries. Questions included personal perceptions of AI knowledge, use, interests and concerns. When asked if they had used AI in the past year, 49 percent of Australians in the survey responded yes. This is slightly above the survey average of 48 percent, and ranks Australia ninth of the 21 countries, noting that there was a great degree of variability between countries (Lohr 2025).
- Using online job advertisements, PwC found that AI demand growth was 36 percent lower than the global benchmark, and the average AI wage premium was 8 percentage points lower than the global average (PwC 2024). It is not clear if this is due to slower adoption by global standards, or if adoption has already matured and growth is as a result slower.
- Stanford University's AI index used LinkedIn data to show that Australia's relative AI skill penetration was slightly below the global average, and alongside the United States, Germany and Great Britain ranked among the least optimistic for AI sentiment (Stanford HAI 2025, pp. 235, 401).

The PC's blueprint for AI regulation

Analysis of potential gaps in current regulation posed by AI must come first

The range of commonly-cited AI risks spans several Australian Government portfolios including health, consumer protection, criminal law, national defence, financial regulation, media regulation and intellectual property. And given the seemingly limitless range of AI applications, all Australian Government agencies should be preparing to adapt to a world with AI. To this end, the Australian Government should undertake a comprehensive set of 'gap analyses' to understand the risks stemming from AI and whether these risks can be dealt with under existing regulatory frameworks.

Such reviews should consider:

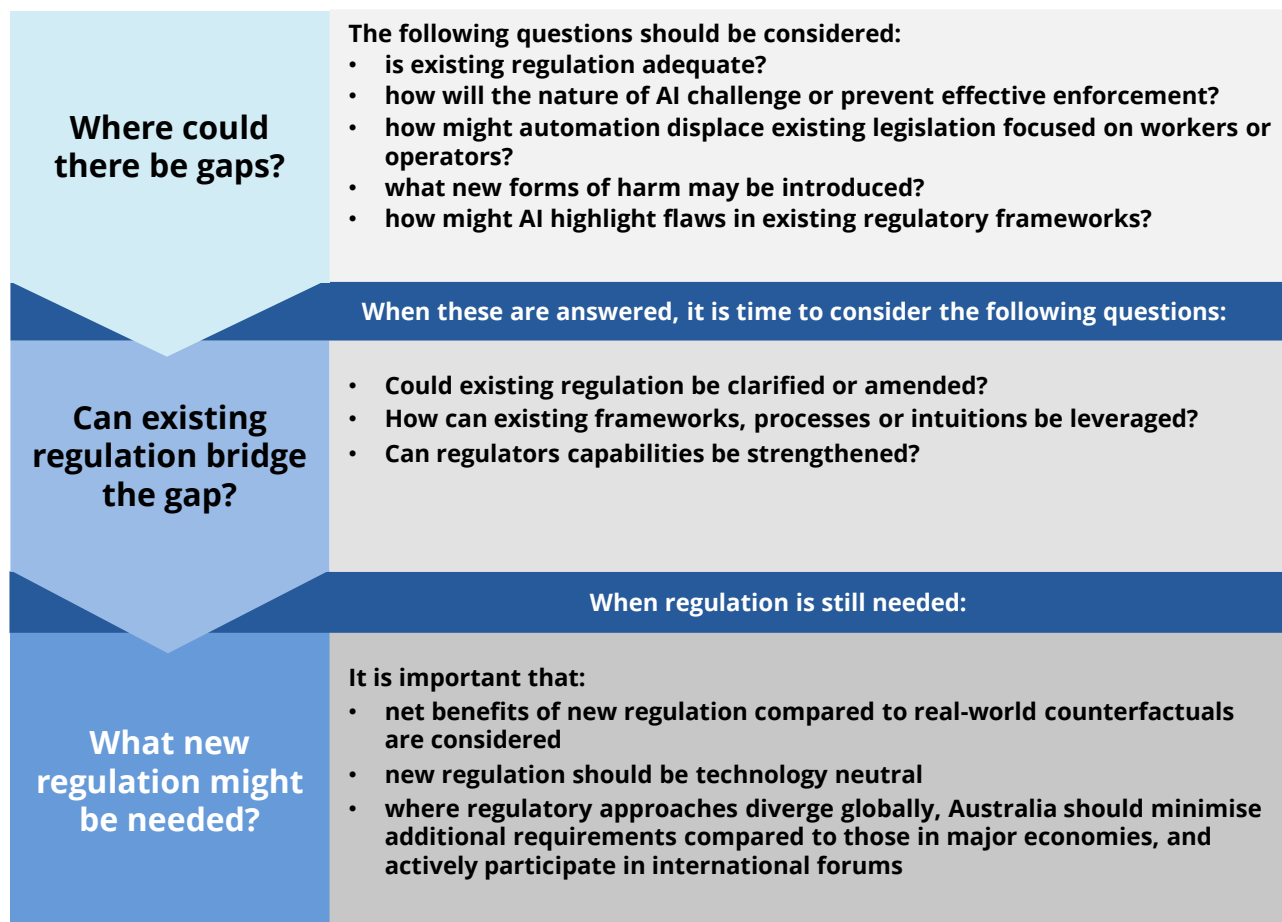
- how AI is being used or is likely to be used in the near future, and whether these uses increase the risk of serious harm compared to what would occur in its absence

- which parties involved have the scope to influence risks and outcomes
- whether the risk is adequately addressed by an existing regulation or whether extensions or modifications to this regulation, or improvements to its enforcement, are required (figure 1.1).

These gap analyses could be conducted by the relevant regulator (in conjunction with policymakers) with existing expertise in the use-cases that are likely to lead to harm. For example, the Therapeutic Goods Administration (TGA) is conducting a review on, among other things, the continuing appropriateness of their existing regulatory approach and requirements for medical devices that incorporate AI.

These gap analyses into the additional risk posed by AI should be completed with urgency, and until they are, consideration of new, economy wide, AI-specific regulations should be paused. This includes the Australian Government Department of Industry, Science and Resources' (DISR) proposed *Mandatory Guardrails for AI in High-Risk Settings* (see below), which would require either modification of existing regulation or potentially new, economy wide legislation to operationalise (three options are proposed in the proposals paper (DISR 2024a, p. 46)). Creating overarching, economy-wide regulations before the gaps in the existing regulatory framework are identified creates the risk of duplication and unnecessarily high compliance burden with little benefit to end consumers.

Figure 1.1 – A range of questions should be answered before regulation is considered



Agencies are already taking the lead in undertaking gap analyses ...

The PC notes that a number of Australian Government agencies have begun AI-focused regulatory gap analyses. Some of the publicly announced inquiries at the federal level include:

- the Department of Health, Disability and Ageing (2024) – has reviewed the potential regulatory responses to the use of AI within the health space (noting both the risks and benefits of AI and the likely uses in the near future)
- the TGA (2024) – has reviewed whether various regulations in its purview are still appropriate given the use of AI in numerous contexts, including in medical devices
- the Treasury (2024) – is reviewing whether the Australian Consumer Law remains suitable to protect consumers who use AI and to support the safe and responsible use of AI by businesses
- the Attorney General's Department (2023a) – has an ongoing reference group to ensure copyright law keeps pace with the challenges posed from AI.

The Department of Health, Disability and Ageing (2025b) has now completed its review. It noted that minor amendments may be needed to clarify legislation in its purview. Likewise, the TGA's (2025) review was released just prior to the publication of this report. This review found that the frameworks for the regulation of medical devices were robust, but incremental changes may be needed to, among other things, ensure definitions used in the *Therapeutic Goods Act 1989* (Cth) are applicable to products using AI. The PC commends the rigour of this review and suggests it be used as a template for future gap analyses.

The two other reviews are either not yet complete or the results have not been made public. The PC is also aware that some agencies are conducting internal reviews, but the existence of these reviews has also not been made public yet.

A number of agencies, such as the Reserve Bank of Australia and the Australian Prudential Regulation Authority, are also monitoring the likely implications of AI, but have not announced public reviews (McCarthy Hockey 2024; RBA 2024).



Draft recommendation 1.1

Productivity growth from AI will be built on existing legal foundations. Gap analyses of current rules need to be expanded and completed.

Australian governments play a key role in promoting investment in digital technology, including AI, by providing a stable regulatory environment. Any regulatory responses to potential harms from using AI must be proportionate, risk-based, outcomes-based and technology-neutral where possible.

The Australian Government should continue, complete, publish and act on ongoing reviews into the potential gaps in the regulatory framework posed by AI as soon as possible.

Where relevant gap analyses have not begun, they should begin immediately.

All reviews of the regulatory gaps posed by AI should consider:

- the uses of AI
- the additional risk of harm posed by AI (compared to the status quo) in a specific use-case
- whether existing regulatory frameworks cover these risks potentially with improved guidance and enforcement; and if not how to modify existing regulatory frameworks to mitigate the additional risks.



Draft recommendation 1.2

AI-specific regulation should be a last resort

AI-specific regulations should only be considered as a last resort for the use cases of AI that meet two criteria. These are:

- where existing regulatory frameworks cannot be sufficiently adapted to handle the issue
- where technology-neutral regulations are not feasible.

Economy-wide efforts to regulate AI should be paused until all gap analyses are complete and implemented

In August 2024 Australian Government Department of Industry, Science and Resources released a set of 10 voluntary AI safety standards, or guardrails, based on risk management standards such as *ISO/IEC 42001:2023 (Information technology – Artificial intelligence – Management system)* and the National Institute of Standards and Technology's *Artificial Intelligence Risk Management Framework (AI RMF 1.0)* (DISR 2024b, p. 5).

The guardrails cover aspects of AI development and application. They require several risk-management processes. These include testing of models, developing a risk plan and providing transparency to users of AI tools and owners of copyrighted materials used in the training of models.

The guardrails outline reasonable risk-management practices for many organisations. In this way they have served a very important and useful step in AI governance in Australia by equipping businesses with voluntary, structured and internationally recognised standards to support and guide their adoption of AI.

The guidelines are very useful for smaller businesses without comprehensive risk-management procedures in place. Indeed, submissions from participants to this inquiry³ (and submissions to the mandatory guardrails – discussed below – consultation process⁴) showed that many larger organisations have implemented risk management protocols that are similar in spirit to these guardrails.

Mandating the guardrails is not necessary

In September 2024 (DISR 2024a) a proposals paper for a set of mandatory guardrails for AI in high-risk settings was released by the Australian Government. The proposal is to turn the voluntary guidelines into mandatory regulations for AI development and application.⁵

The PC is concerned with two aspects of the guardrails being made *mandatory*. First, the proposals paper argued that the mandatory guardrails would apply to all high-risk uses of AI – regardless of whether risks can be better mitigated through outcomes-based regulations. Second, the proposals paper argued that General Purpose AIs – which would include many generative AI tools – above a certain threshold of capability be classified as high risk by default. The proposals paper did not argue for any particular measure or threshold

³ Atlassian (qr. 50, p. 8); Intuit Australia (qr. 36, pp. 9–11); KPMG (qr. 60, p. 3); Microsoft (qr. 52, p. 5); Salesforce (qr. 57, p. 5); Workday Australia (qr. 56, p. 6)

⁴ (Accenture 2024b, p. 3; Commonwealth Bank of Australia 2024b, p. 3; IBM Australia 2024, p. 1; Indeed 2024, pp. 2–3; LinkedIn 2024, pp. 4–5; Mastercard 2024, p. 1; RMIT University 2024, p. 1; SEEK Limited 2024, pp. 3–4; Telstra 2024a, pp. 4–5; The University of Melbourne 2024, p. 3)

⁵ The mandatory guardrails do differ from the voluntary guardrails slightly in that while the tenth mandatory guardrail requires conformity assessments to demonstrate and certify compliance with guardrails, the tenth voluntary guardrail requires engagement and consultation with stakeholders (DISR 2024a, p. 35, 2024b, pp. iv, 13–14).

for technical capability, though it could include aspects like FLOPS⁶ (DISR 2024a, p. 18). It was argued that these models can perform so many functions that their risks cannot be adequately foreseen. This could result in the guardrails being applied to common generative AI tools such as ChatGPT, Claude and Grok, depending on what is chosen as the threshold and measure of technical capability.

In general, high-risk uses of AI can be split into three broad types.

1. *High risk uses that can be adequately controlled by existing regulatory frameworks* (potentially with some modification) – this could include issues with privacy law (which the PC thinks can be resolved within existing frameworks with modification to make the regulations more outcomes focused, chapter 2).
2. *High risk uses that can be adequately controlled with new technology-neutral regulations* – this could include (non-consensual) sexually explicit deepfake images which the Australian Government has recently banned (through the *Criminal Code Amendment (Deepfake Sexual Material) Act 2024*).⁷
3. *High risk use cases that require technology-specific regulations* – these would be use cases identified in the various gap analyses as having no technology-neutral solution.

The PC's concern with the guardrails is that they would not distinguish between these categories. This in our view raises significant issues, as the first two cases can already, by definition, be dealt with adequately by other regulatory mechanisms. It might also result in most commercial chatbots being classified as high risk regardless of the efficacy of existing regulations. The result of this approach is that many AI models would be complying with two different sets of regulation to achieve the same outcome.

For example, the TGA's review noted that with respect to medical devices, all ten proposed guardrails had close parallels in existing regulations (2025, pp. 27–30). That is, it is likely that firms providing AI-based medical devices in Australia would already be fulfilling the objectives of the guardrails if they are operating legally under the TGA's existing regulations. But if the guardrails are mandated, then the provider of the medical device would need to demonstrate compliance with the TGA regulations *and* the guardrails, raising the regulatory burden with no change in outcomes.

The mandating of the guardrails is only appropriate in circumstances where existing regulatory frameworks or new technology-neutral regulations are not able to adequately mitigate the risk of harm. Once the Australian Government has completed and acted on all gap analyses of its existing policy framework, it will know what regulatory holes cannot be plugged by existing frameworks or new technology neutral legislation. Consideration of economy wide efforts to mandate the guardrails should be paused until these gap analyses are complete.



Draft recommendation 1.3

Pause steps to implement mandatory guardrails for high-risk AI

The Australian Government should only apply the proposed 'mandatory guardrails for high-risk AI' in circumstances that lead to harms that cannot be mitigated by existing regulatory frameworks and where new technology-neutral regulation is not possible. Until the reviews of the gaps posed by AI to existing regulatory structures are completed, steps to mandate the guardrails should be paused.

⁶ FLOPS here refers to a measure of the number of calculations a system can perform in a second. A higher FLOPS AI system is therefore capable of completing more complex tasks (Pressley 2023).

⁷ The Criminal Code Amendment (Deepfake Sexual Material) Bill 2024 actually bans the sharing of *any* sexual image or video (real or fake) without consent (s. 474.17A of the Criminal Code Act 1995).

Are there risks of waiting for gap analyses before taking regulatory action?

New, untested, guardrails are more likely to raise uncertainty than lower it

The proposals paper for mandatory guardrails for AI argued that ‘regulatory clarity and certainty for those developing and deploying AI is essential’ and said that the proposed mandatory guardrails aim to ‘provide businesses with greater regulatory certainty’ (DISR 2024a, p. 2). Certainty is important for business but new regulations, such as the guardrails, that may need to be tested before the courts and overlap with other existing regulations may raise, not lower, regulatory uncertainty. They will also raise regulatory costs.

For example, Westpac stated that the ‘financial services industry is already subject to extensive regulatory requirements, many of which will apply where AI is used’ (2024, p. 3) and that a ‘regulatory regime that is overly burdensome will have negative impacts on innovation and the productivity benefits that this technology brings, while also hindering Australia’s ability to compete internationally’ (2024, p. 4).

A sound way for the Australian Government to mitigate regulatory uncertainty would be to express a strong preference for regulatory changes to be technology-neutral, risk-based and within existing frameworks, while stating that technology-specific regulation will only be used as a last resort. This would help limit the negative effect on innovation as stakeholders can (with high likelihood) rule out the possibility of costly economy-wide AI regulation taking effect. And by making it clear that the Australian Government retains the option of technology-specific regulation as a last resort, they would not lock out any regulatory options in the future.

The current guardrails process is intended to be risk-based but the proposal paper did not express a clear preference for being technology-neutral or being based within existing regulatory frameworks. A further discussion paper that expresses such a strong preference may help mitigate any deterrence on investment.

Australia’s regulatory response to AI should be consistent with overseas peers

International regulatory approaches to AI are likely to greatly influence the regulatory landscape in Australia and there are sound reasons for us to be a ‘regulation taker’ in this area (PC 2024e, p. 9). A large amount of AI technology used in Australia is imported from overseas, and most domestic producers have a strong interest in making their products available to overseas markets.

At present, there appears to be no international consensus on how to approach AI regulation, and technology-specific regulation is still rare (table 1.1). The main jurisdiction that has enacted AI-specific regulation is the EU with its AI Act. But since the passage of this legislation there have been few signs that the rest of the world will follow suit. Japan has also introduced AI-specific regulation, but it appears to impose minimal responsibilities, and it does not include any enforcement measures. Canada too introduced a Bill into the Canadian Parliament that would have introduced AI-specific regulation. The Bill stalled in parliament ahead of Canada’s federal election in early 2025 and as at July 2025 there is no new information on whether the process will restart or if a new Act will be considered (Fraser and Anderson Dykema 2025). Indeed, most other countries have not opted to regulate AI directly but instead have chosen to rely on existing regulatory frameworks.

That said, Australia should continue to be an active participant in international forums that aim to create consistent AI standards and approaches. As a ‘regulatory taker’, Australia needs to make sure its interests are strongly represented in these forums and that any outputs and agreements are consistent with Australia’s interests and support our productivity growth.

Table 1.1 – AI specific regulation is relatively rare globally**Notable examples of regulation that have been enacted or raised in parliament**

Regulation	Details	Status
European Union: AI Act	The AI Act is part of a wider set of policy measures to guarantee safety and strengthen AI uptake (European Parliament 2023c). The Act is risk-based and defines 4 levels of risk: unacceptable risk, high risk, limited risk and minimal risk. New bodies are required to enforce the Act and there are a set of obligations (with some activities banned outright) that sit under each risk level (European Parliament 2023a).	The AI Act entered into force in August 2024, and all elements of the legislation will come into force in August 2026. The prohibitions that apply from February 2025 and the rules for high risk systems have an extended transition period until August 2026 (European Parliament 2023a). There has been media coverage suggesting that some elements of the Act (that are yet to kick in) may be paused (Leprince-Ringuet and Partington 2025). Some technical standards have yet to be developed, and exemptions for SMEs and some low complexity AI systems are being considered (DLA Piper 2025). The possible pause follows industry pressure on the EU over its regulatory approach.
United States: State-based legislation	There is no US-wide AI regulation. ^a However, some states have introduced their own AI-related legislation or resolutions (Taylor et al. 2025). Given that many of the companies developing AI are based there, California's regulatory approach may be the most impactful.	The Californian regulation applies only to AI developers, and developers must comply with it by January 2026. Many of the requirements are related to disclosure, for example providing information on datasets used in AI processes (Kourinian 2024).
Canada: Artificial Intelligence and Data Act	The Act planned for a staged implementation. Initially, the aim was to be on education and establishing guidelines, allowing the ecosystem to adjust to the new framework before enforcement actions are undertaken (Government of Canada 2025). Much like the EU Act, it had a planned focus on high-impact systems, with obligations on seven classes of AI uses.	The Act stalled in parliament before the country's federal election in early 2025. (Fraser and Anderson Dykema 2025). As at July 2025 there is no new information on whether the process will restart or if a new Act will be considered (Duball 2025).
Japan: Act on Promotion of Research and Development and Utilization of Artificial Intelligence-Related Technologies	An Act will establish core principles for the development and use of AI and an AI Strategy Centre. Many of the provisions in the Bill are related to goals rather than legislative requirements. It gives the AI Strategy Centre the ability to request cooperation from entities as necessary, but there are no penalties for failing to comply (White & Case 2025).	On 28 May 2025, the Bill was approved by Japan's Parliament. The government is considering creating an ability to publicly name companies that do not co-operate, but this was not included in this Bill (White & Case 2025).

a. The PC notes that the US Government has released an AI Action Plan and the US President has signed three accompanying executive orders to implement this plan. This plan includes, inter alia, efforts to remove regulatory barriers to AI uptake and development at the Federal level (The White House 2025d, 2025a, 2025c, 2025b).

Case study: copyright law in the age of AI

Copyright violation is an example of a harm that AI could exacerbate by changing economic incentives. Previous waves of innovation in information and communication technology have made the sharing of copyrighted materials much cheaper and easier, creating challenges for copyright. In most instances, copyright law was able to be adapted (or better enforced) to mitigate the harm. This made it unnecessary to directly regulate technology by, for example, regulating computer software or hardware to prevent copyright breach.

It is the PC's view that the copyright issues posed by AI can also similarly be resolved through adapting existing copyright law frameworks rather than introducing AI-specific regulation.

What is copyright?

Copyright law prohibits a person from using original works without the permission of the copyright holder – usually the author (AGD 2022a). The types of works that are protected include text, artistic works, music, computer code, sound recordings and films (ACC 2024a). It does not protect the underlying ideas or information (AGD 2022a). In some cases, data and datasets may be protected, 'largely depend[ing] on how the data has been arranged, structured or presented' (Allens 2020, p. 3).

The rise of AI technology has led to new challenges for copyright law.

The emergence of AI also raises some additional, principle-based questions about how the copyright framework (as part of Australia's broader intellectual property regime) works to benefit society by encouraging creation and innovation, rewarding intellectual effort and achievement, and supporting the dissemination of knowledge and ideas. (AGD 2023c, p. 12)

In 2023, the Attorney-General established the Copyright and Artificial Intelligence Reference Group, which acts as 'a standing mechanism to engage with stakeholders across a wide range of sectors on issues at the intersection of AI and copyright' (AGD 2023a). Since then, the group has met on several occasions to discuss issues relating to AI technology and copyright law (AGD 2023a).

This section explores one issue particularly relevant to productivity: whether current Australian copyright law is a barrier to building and training AI models. There are other legal issues relating to the outputs of AI models that are less relevant to productivity – such as whether those outputs attract copyright protection and what happens when AI outputs infringe a third party's copyright (Evans et al. 2024).

Training AI models

Building and refining AI models requires the use of large amounts of data.

The term 'AI model training' refers to this process: feeding the algorithm data, examining the results, and tweaking the model output to increase accuracy and efficacy. To do this, algorithms need massive amounts of data that capture the full range of incoming data. (Chen 2023)

The datasets used to train AI models often contain digital copies of media such as web pages, books, videos, images and music. These media are often the subject of copyright protection, which means that their use to train AI models requires permission from the copyright holder. Permission is required because AI models must 'copy' the protected material at least temporarily to undertake the training process. The use of copyrighted materials to train an AI model is a separate issue to the copyright status of anything the model produces. As discussed above, AI outputs may have their own copyright challenges.

A survey of the Copyright and Artificial Intelligence Reference Group indicated that, in practice, a range of copyrighted materials are used to train AI models – including literary and artistic works, sound recordings, films and musical works (AGD 2024, p. 12).

There is evidence to suggest that large AI models are already being trained on copyrighted materials without consent or compensation (APA and ASA, qr. 39, pp. 3–4; APDG, qr. 6, p. 4; APRA AMCOS, qr. 58, p. 4; ARIA and PPCA, qr. 65, p. 5, Creative Australia, qr. 62, p. 3). It should be noted that Australian copyright law only applies to copying that occurs within Australia's boundaries – in other words, the training of AI models overseas is subject to the relevant laws of the jurisdiction in which it occurs. Lawsuits have been brought against technology companies – including Meta, Microsoft and OpenAI – in some overseas jurisdictions about the unlicensed use of copyrighted works to train AI models (Ryan 2023).

There are concerns that the Australian copyright regime is not keeping pace with the rise of AI technology – whether because it does not adequately facilitate the use of copyrighted works or because AI developers can too easily sidestep existing licensing and enforcement mechanisms. There are several policy options, including:

- no policy change – that is, copyright owners would continue to enforce their rights under the existing copyright framework, including through the court system
- policy measures to better facilitate the licensing of copyrighted materials, such as through collecting societies
- amending the Copyright Act to include a fair dealing exception that would cover text and data mining.

The PC is seeking feedback on what reforms are needed to bring the copyright regime up to date.

Is there a need to bolster the licensing or enforcement regime?

Several participants expressed concern about the unauthorised use of copyrighted materials to train AI models. For example, Creative Australia said:

Much of the data has been used reportedly without consent from the original creator, and without acknowledgement or remuneration. The global nature of the technology industry has made it difficult for the owners of creative work to enforce their intellectual property rights and be remunerated for the use of their work. (qr. 62, p. 3)

There are two points at which concerns of this type could be addressed. First, they could be addressed before the fact, through copyright licensing. Licensing is the key mechanism through which a copyright holder grants permission for others to use their work and often involves some form of payment. In Australia, licensing is often done through collecting societies, which are organisations that represent copyright holders. This can streamline the licensing process, because the collecting society can negotiate licences on behalf of multiple copyright holders at once. As the Copyright Agency said:

We can help these sectors use third party content for AI-related activities. Our annual licence for businesses now allows staff to use news media content in prompts for AI tools (e.g. for summarisation or analysis). We are extending this to other third party content later in the year. We are also in discussions with our members and licensees about other collective licensing solutions, including the use of datasets for AI-related activities. (qr. 7, pp. 2–3)

The issue of unauthorised use of copyrighted materials could also be addressed after the fact, through enforcement. This encompasses a range of possible measures, including take-down notices, alternative dispute resolution and court action. In 2022-23, the Attorney-General's Department undertook a Copyright Enforcement Review to assess 'whether existing copyright enforcement mechanisms remain effective and

proportionate' (AGD 2022b). That review found that additional regulatory measures are needed to achieve an effective copyright enforcement regime, and work is currently underway to identify options for:

- reducing barriers for Australians to use of the legal system to enforce copyright, including examining simple options to resolve 'small value' copyright infringements
- improving understanding and awareness about copyright. (AGD 2023b)

In light of this ongoing work, the issue of copyright enforcement is not in scope for this inquiry.

Is there a case for a text and data mining exception?

Another option is to expand the existing 'fair dealing' regime, which provides certain exceptions to the requirement to obtain permission from the copyright holder (box 1.6). Currently, there is no exception that covers AI model training per se (The University of Notre Dame Australia 2024). However, depending on the case, a different exception could apply. For example, AI models built as part of research could fall within the scope of the 'research or study' exception.

Box 1.6 – What are fair dealing exceptions?

Fair dealing exceptions allow for the use of copyright material without permission from the copyright owner, so long as it is used for one of several **specified purposes** and is considered **fair**.

What are the specified purposes?

The Copyright Act specifies several purposes where the exception may apply. These include: research or study, criticism or review, parody or satire, reporting news, and enabling a person with a disability to access the material (*Copyright Act 1968* (Cth), Part III, Div 3; Part VIA, Div 2).

What counts as 'fair'?

Fairness is determined with regard to all the relevant circumstances – that is, it depends on the facts. Some purposes have specified criteria that must be taken into account. For example, where the use is for research or study, the following considerations apply:

- the purpose and character of the dealing
- the nature of the work
- whether the work can be obtained within a reasonable time at an ordinary commercial price
- the effect of the dealing upon the potential market for, or value of, the work
- how amount and substantiality of the work that was copied (*Copyright Act 1968* (Cth), s 40(2)).

The 'fair use' doctrine – an alternative approach

Some overseas jurisdictions (notably the United States) take a 'fair use' approach to copyright exceptions. Under this doctrine, *any types of use* can be considered non-infringing, provided that it is considered 'fair' – in other words, the use need not fall within one of several defined categories. Several reviews have recommended the adoption of the fair use doctrine in Australia (including by the Australian Law Reform Commission and the Productivity Commission), but this has not occurred.

Source: ACC (2024b); ALRC (2013); *Copyright Act 1968* (Cth); PC (2021, p. 187).

In its report on *Copyright and the Digital Economy*, the Australian Law Reform Commission recommended amendments to enable text and data mining by adopting a fair use approach to copyright exceptions (box 1.6) – or, failing that, through a new fair dealing exception. It explained:

There has been growing recognition that data and text mining should not be infringement because it is a 'non-expressive' use. Non-expressive use leans on the fundamental principle that copyright law protects the expression of ideas and information and not the information or data itself (2013, p. 261)

The Australian Government has since indicated that it is not inclined to introduce a fair use regime (Australian Government 2017, p. 7). Therefore, the PC is considering whether there is a case for a new fair dealing exception that explicitly covers text and data mining (a 'TDM exception'). TDM exceptions exist in several comparable overseas jurisdictions (box 1.7).

Such an exception would cover not just AI model training, but all forms of analytical techniques that use machine-read material to identify patterns, trends and other useful information. For example, the use of text and data mining techniques is common in research sectors to produce large datasets that can be interrogated through statistical analysis.

Box 1.7 – Text and data mining around the world

European Union: There are two text and data mining (TDM) exceptions embedded in the Digital Single Market Directive (EU 2019/790) – one for scientific research (article 3) and another for general use (article 4). The Artificial Intelligence Act (Regulation (EU) 2024/1689) specifically characterises the training of AI models as involving 'text and data mining techniques' (recital 105) and refers to the TDM exception (article 53). The recent case of *Kneschke v. LAION* [2024] endorsed the view that the TDM exception extends to cover AI training (Goldstein et al. 2024a, 2024b).

United States: It has been argued that training AI models falls within the scope of the fair use doctrine (Khan 2024; Klosek and Blumenthal 2024). However, the case *Thomson Reuters v. Ross* [2023] 694 F.Supp.3d 467 highlights that whether AI training is covered by the doctrine depends on whether the fair use factors are met in the circumstances (ReedSmith 2025).

United Kingdom: There is a TDM exception for that applies to non-commercial research (UK Intellectual Property Office 2014). There have been proposals to expand the exception to cover all uses, though these are still under consideration (Pinsent Masons 2023; UK Government 2024).

Japan: The Japanese Copyright Act includes broad statutory exemptions for TDM (article 30-4(ii)), provided the work is used for 'non-enjoyment' purposes (Senftleben 2022, p. 1494). In essence, the requirement for 'non-enjoyment' distinguishes between whether the work is being consumed as a work or as data, and is broadly equivalent to the distinction between expressive and non-expressive uses.

Singapore: The Singaporean Copyright Act includes a specific TDM exception, as well as a broader fair use exception (Ng-Loy 2024).

To assist its consideration of this option, the PC is seeking feedback about the likely effects of a TDM exception on the AI market, the creative sector and productivity in general – particularly in light of the following considerations.

- At present, large AI models (including generative AI and large language models) are generally available to be used in Australia. The introduction (or not) of a TDM exception is unlikely to affect whether AI models continue to be available and used in Australia (PC 2024c, p. 13).
- At present, large AI models are trained overseas, not in Australia. It is unclear whether the introduction of a TDM exception would change this trend.
- As discussed above, large AI models are already being trained on unlicensed copyrighted materials.
- A TDM exception could make a difference to whether smaller, low compute models (such as task-specific models) can be built and trained in Australia, such as by Australian research institutions, medical technology firms, and research service providers.

It should also be noted that a TDM exception would not be a ‘blank cheque’ for all copyrighted materials to be used as inputs into all AI models. As discussed in box 1.4, the use must also be considered ‘fair’ in the circumstances – this requirement would act as a check on copyrighted works being used unfairly, preserving the integrity of the copyright holder’s legal and commercial interests in the work. There may be a need for legislative criteria or regulatory guidance about what types of uses are likely to be considered fair.



Information request 1.1

The PC is seeking feedback on the issue of copyrighted materials being used to train AI models.

- Are reforms to the copyright regime (including licensing arrangements) required? If so, what are they and why?

The PC is also seeking feedback on the proposal to amend the *Copyright Act 1968* (Cth) to include a fair dealing exception for text and data mining.

- How would an exception covering text and data mining affect the development and use of AI in Australia? What are the costs, benefits and risks of a text and data mining exception likely to be?
- How should the exception be implemented in the Copyright Act – for example, should it be through a broad text and data mining exception or one that covers non-commercial uses only?
- Is there a need for legislative criteria or regulatory guidance to help provide clarity about what types of uses are fair?

2. New pathways to expand data access

Summary

- * **When individuals and businesses can access and share data that relates to them, they can get more value from the products and services they use and more easily try new ones. They can also access useful insights and advice to make better decisions. These benefits can boost innovation and competition, potentially adding up to \$10 billion a year to the economy through productivity growth.**
- * **The benefits of data sharing remain somewhat untapped in Australia, as data access for consumers remains patchy and inconsistent across the economy.**
 - Individuals and businesses often resort to unofficial data access tools (such as screen scraping) which can be unreliable and insecure. Use of these tools can result in legal sanctions, and increased cybersecurity, privacy, and consumer protection risks.
- * **The Australian Government has implemented some significant, but disjointed policies to improve data access, including the Consumer Data Right (CDR), My Health Record and more recently, the Motor Vehicle Service and Repair Information Sharing Scheme.**
 - The CDR has made strong progress in banking and energy after a slow and bumpy start. But its accreditation model, bespoke privacy safeguards, and technical requirements are too onerous for most sectors – despite its design as an economy-wide framework.
- * **The Australian Government should establish lower-cost and more flexible regulatory pathways to expand data access for individuals and businesses.**
 - The pathways could create a simple, tiered approach to data access where the obligations on data holders and the level of government involvement can match the needs and digital maturity of different sectors.
 - This could include an industry-led data pathway for basic ‘snapshot’ access to relatively non-sensitive data and a standardised data transfer pathway that includes core technical requirements that can support high- frequency data transfers and interoperability.
 - The pathways would ‘meet sectors where they are’ and be gradually implemented over the next decade to give individuals and businesses more consistent and useable access to data across the economy.
- * **Pathways for data access should begin with data where the sharing is of high benefit but relatively low cost; and there is clear value to consumers.**
 - The Australian Government should assign an appropriate body to assess the digital and data ‘readiness’ of individual sectors focusing, in the first instance, on identifying opportunities to enhance data access where there are large potential benefits and/or low marginal compliance costs.
 - Potential early use cases include in the area of telematics applied to agricultural equipment, supermarket loyalty data and access to information for renters.

Data about you should be available for you to use

Every day, data about you is created and put to valuable uses across the economy. The volume of data produced has increased exponentially within the last few decades and new technologies – such as artificial intelligence (AI) – unlock new uses for this data. The retail share of e-commerce has grown from less than 3% to more than 11% since 2013 (ABS 2024d), and growth will likely continue (PC 2024c). This data is monetised, traded and shared with other parties (Fernandez et al. 2020, p. 11). But often you, the data subject, cannot easily access data about yourself. So, while individuals and businesses do have better access to some of the data that is collected and held about them than they did a decade ago, much of it remains invisible to them or unusable (Deloitte 2024a, p. 15).

Better data access will benefit people and businesses and promote competition and innovation across the economy (Jones 2024b). Easier access to the data that relates to you – and the ability to share it with trusted third parties – could lead to more personalised, innovative services that boost productivity and can help you make better decisions. For instance, health data can empower consumers to take an active role in managing their care (ADHA, qr. 16, p. 4), and consumption data can help individuals to understand and optimise their spending on and use of products and services (EnergyFlex 2025; WeMoney 2025). Autonomous AI agents can handle tasks for consumers, but getting value from these technologies often relies on data access (DTI 2024b, pp. 83–88).

For businesses, data access unlocks an analogous set of benefits. Firms can use data to identify business process improvements, facilitate automation and provide innovative new services for consumers (O'Mahoney et al. 2022, p. 9). Effective use of data is correlated with higher revenue growth (O'Mahoney et al. 2022, p. 2). Open banking initiatives internationally have been linked to greater fintech entry (Babina et al. 2025, p. 1) and can increase investment by making it easier for lenders to review loan candidates and by expanding credit access for borrowers (CFIT 2024, p. 8).

Australia needs to improve the state of data access to unlock this untapped value. While initiatives around banking, health and energy data are delivering some value in Australia, these initiatives are far from mature (Jones 2024b; PC 2024a, p. 15). In the future, productivity gains from greater data sharing could be on the order of \$1 billion to \$10 billion (appendix B).

What is the current state of data access?

The types of data that is captured about individuals and businesses through the products and services they use varies extensively across the economy (box 2.1). And there is little to no consistency across, or even within, different sectors, about which parts of these data holdings individuals and business can access.

As digital customer accounts and portals have become common, and often obligatory, consumers more often have some form of direct access to the basic information they have given to a product or service provider. Businesses and organisations that are subject to the Privacy Act must provide individuals with access to their personal information upon request (chapter 3) (OAIC 2023b). Individuals and businesses can often access some amount of the transaction or activity history data from the products and services they use. For example, Qantas' Frequent Flyer program allows members to download activity statements and Woolworths Rewards and Flybuys allow members to download 'eReceipts' in Portable Document Format (PDF) form (Coles 2025; Everyday Rewards 2025; Qantas Money 2025).

Box 2.1 – What do we mean by data access?

The way data originates affects who knows about it, who can control it, and how it can be used. Data may be provided directly by individuals and businesses (volunteered), captured or recorded from their activities (observed), obtained from third parties (acquired) or produced by transforming (e.g. date of birth to age) existing data (derived) or applying analytics to predict or estimate (e.g. credit scores) other data points (inferred) (OECD 2019, p. 29).

This reform focuses on data that can be identified with an individual person or business (**consumers**). This includes data that is about or describes an individual or business (e.g. age, address, revenue) or relates to the products and services they use (e.g. loyalty points, viewing history, device runtime).

In this chapter **data access** refers to the ability of consumers to view, share, bundle, modify and otherwise use data that is held by the providers (**data holders**) of the goods and service they use. Data holders include both private and public sector entities that control data relating to consumers, regardless of whether they 'collected, stored, processed or disseminated' the data themselves (OECD 2019, p. 35).

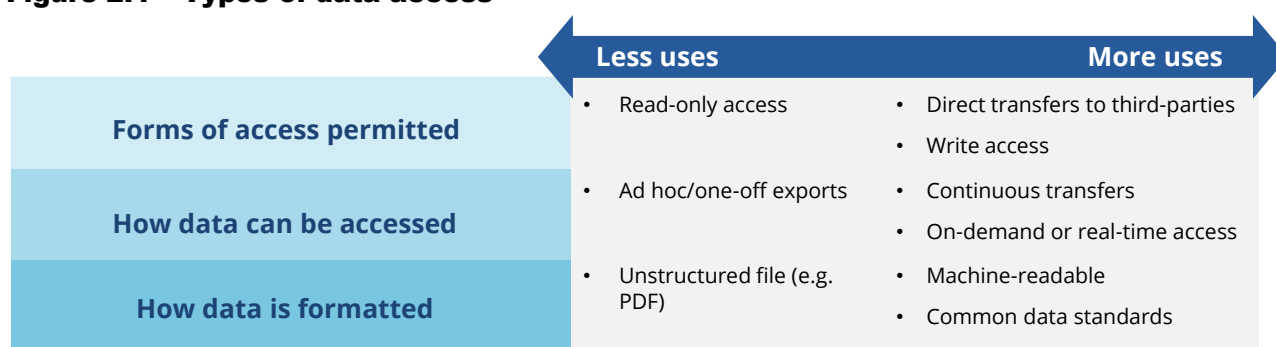
However, in other sectors consumers lack basic access to data about themselves from the products and services they use. It can be particularly difficult for individuals to access data from government funded services (including in the health and care sectors).

- Optometrist customers can struggle to share their previous eye exam results and detailed prescription information. Incompatible diagnostic equipment and systems and non-standard file formats affect how seamlessly records can be used by, and transferred to another optometrist (Optometry Australia 2024).
- While nearly all pharmacies use the My Health Record (MHR) system, non-prescription medicines are not automatically uploaded (PC 2024a). The Pharmacist Shared Medicines List is intended to give health professionals a complete snapshot of all medicines a consumer is taking to help safely manage complex conditions (Digital Health 2019). But it is only currently supported by a small number of software vendors and industry sources report that awareness and uptake remains low (Elliott et al. 2024).

Not all data access is equal

Three key factors influence how usable and useful data is for individuals and businesses: what forms of access are permitted, how data can be accessed, and the format of the data (figure 2.1).

Figure 2.1 – Types of data access



Data that is provided in an unstructured form (e.g. PDF) or on a read-only basis (e.g. an in-app dashboard) is typically harder to make use of – it will often need to be copied out, transformed and then manually uploaded elsewhere (FormX 2025). In contrast, allowing people to share data about themselves with third parties of their choosing in a standardised format can support high-value use cases (OECD 2024b, p. 6). These third parties may be providers of competing or related products and services, intermediaries that collate and manage data across disparate sources or third-party providers that use the data to provide personalised advice and insights (CCAF 2024, p. 17; CDEI 2022, pp. 8–9).

The experience of Australia's Consumer Data Right (CDR) – a government administered sharing scheme – is illustrative of how difficult it can be to build and administer a comprehensive data sharing regime that meets the many demands of different users efficiently and cost effectively (box 2.2). The scheme currently operates in the banking and energy sectors and allows customers to send fine-grained transaction data directly to Accredited Data Recipients via secure, standardised Application Programming Interfaces (APIs). This functionality is used by a suite of apps that assist consumers with personalised budgeting (e.g. Frollo), accessing financial services (e.g. WeMoney) and improving their household energy efficiency (e.g. EnergyFlex) (Open Finance ANZ 2025, p. 18). But the CDR's bespoke privacy rules mean any data obtained, or even derived, from the scheme remains tightly restricted, limiting onward sharing (Treasury 2023b, p. 3). For instance, Xero – a widely used cloud-based accounting platform – has not yet sought accreditation as a data recipient because the CDR's rules would prevent its customers from sharing data and insights accessed through the scheme to advisors of their choosing (Xero 2022, p. 5, 2024, p. 2)⁸.

Box 2.2 – CDR is making headway after a slow and bumpy start

The **Consumer Data Right** (CDR) was established under Part IVD of the *Competition and Consumer Act* and introduced in 2019, allowing consumers to consent to the transfer of their data to accredited third parties within designated sectors. It aimed to enhance competition and innovation by facilitating greater access to consumer data (Jones 2024b). This would help consumers access better products, lower prices, and third-party apps.

The scheme has proved costly and complex to implement. A significant driver of costs has been its binding data standards that have continuously been revised (Treasury 2023b, p. 3). Since the rollout in mid-2020, there have been over 20 versions of the binding CDR data standards. As of 2024, the banking industry reports that it has spent \$1.5 billion on CDR, with implementation costs for data holders ranging from under \$1 million to well over \$100 million each (Accenture 2024a; Treasury 2023b, pp. 2–3).

Despite this, the CDR is making headway, with its expansion into energy having progressed more smoothly. Recent rule changes have streamlined the operational processes for CDR participants, while easing the compliance burden. In the six months to June 2024, it was reported that around 226,000 consumers across the Australian economy used the CDR. By mid-October, more than 300,000 ongoing data sharing arrangements were in place (ACCC 2024c). Use cases have grown to 197, and while lending, credit and broking use cases lead the way, a more diverse range of use cases have entered the ecosystem (Open Finance ANZ 2025, pp. 5, 17).

⁸ Xero has bilateral agreements with banks that enables customers to connect their bank and pull transaction data into their Xero account via a secure, encrypted connection (Xero 2025).

Nonetheless, data access in adjacent sectors can be far more limited. For example, superannuation funds typically limit members to downloading non-machine-readable PDF statements (or, at best, export limited comma separated values (CSV) files for advisers) (ART 2025; Expand 2025). Private health insurers often only show benefit usage in portals without any option to export the underlying data.

In general, digital platforms and technology firms tend to be better at providing users with access to more of the data they hold about them in a usable form. For instance, Facebook's 'Download Your Information' tool lets users export posts, photos, messages and ad clicks (Facebook 2025). Some enable users to directly transfer their device data to another service, for example – Fitbit, Apple Watch and Garmin allow users to sync their activity data (daily steps, heart rate, etc) to third-party platforms such as Strava (Allison 2025; Scott 2024). But these same businesses usually withhold user data that they can use to generate revenue or differentiate themselves from competitors (Deloitte 2023, p. 16; OECD 2021c). This includes granular event level data (such as click-streams) and value-added 'inferred' data (such as ad and taste-profile scores). For example, Fitbit, Apple and Garmin do not permit users to export the raw accelerometer data from their devices or reveal the parameters behind their proprietary 'fitness scores' (White et al. 2024, p. 2).

Hidden in plain sight: the material costs of data access constraints

When providers make it difficult to access data, individuals, businesses and data intermediaries often 'find a way' via unofficial tools and methods (CCAF 2024, p. 20; OECD 2021b, p. 13). There is a diverse ecosystem of third-party devices and software solutions that help consumers independently capture or tap into data from the products and services they use (table 2.1). Many require consumers to pay for add-on hardware or on-going subscription fees to use them, underscoring the demand for data access.

Table 2.1 – Alternative data access tools and methods

	Access method	Examples	Drawbacks
Reverse engineered APIs	Replicates the functionality of a data holder's APIs which have not been published for external use. These 'backdoor' solutions are often made by hobbyists and user advocates.	MyShopDash is a small Australian browser-extension that allows user to export item-level data from their e-receipts in supermarket portals (e.g. Woolworths, Coles) into machine-readable files and visualisations.	Can be unreliable if they fail to perfectly replicate the original system's data handling mechanisms (such as when a vendor updates their firmware)
Screen scraping	Extracts data from the visual interface of a website or app. It involves programmatically simulating user interactions and then extracting the content.	Used by fintech and personal finance management tools to import account data not available through the CDR (e.g. superannuation and share portfolios)	Requires users to share their login-credentials. Changes to an interfaces' design can break the scraping process, resulting in extraction failures.
Scrobbler services	Automatically logs user activity or content consumption (e.g. media played) in real time, often via APIs or apps that track usage and transmit to a logging service.	Trakt.TV and Last.fm track the content that users view or listen to across streaming services (e.g. Spotify, iTunes, Netflix) to compile searchable logs and generate recommendations and personalised profiles that can be ported across platforms.	Requires extensive browser read permissions to function and can miss activity not captured by the device or app.
Add-on monitors and 'data loggers'	Hardware devices that plug into systems (e.g. vehicles, electricity meters) to read diagnostic or operational data from onboard sensors or digital interfaces.	Catch Control is an Australian energy use monitor that 'clamps' onto home switchboards to capture solar production, grid import/export and load data which can be streamed into an analytics app and used to optimise systems.	Requires purchasing and installing the monitor. Some products will not have accessible ports that a monitor can be plugged into.

Source: Catch Power (2025); CCAF (2024, p. 20); Last.fm (2025); Leung (2022); MyShopDash (2025); Trakt.TV (2025); Treasury (2023c, pp. 5–6).

The use of alternative data access tools can sometimes fall into legal grey zones. Section 47D of the *Copyright Act 1968 (Cth)* allows developers to reproduce some parts of a computer program to create new software that can integrate with it. However, if a tool reproduces software beyond what is allowed, bypasses security controls or breaches terms of service, it may run afoul of privacy, copyright or other laws.

Because these tools can undermine the ability of original providers to monetise or otherwise gain advantage from the data they control, they will often try to deter or prevent their customers from using them (Castro and Steinberg 2017, p. 1). This can take the form of technical blocks (e.g. disabling access ports or throttling connection speeds), imposing paywalls (e.g. to access an API) or legal sanctions (including declaring terms of service violations and voiding product warranties). But they can also spur data holders to improve their service offerings. For example, Apple's iPhone 'screen time' tracker was introduced in 2018 to compete with the proliferation of third-party apps that used reverse-engineered analytics and remote access software to allow users to access app usage statistics and set app limits (Nicas 2019).

Relying on insecure and unreliable data access methods

The use of alternative data access tools can increase the likelihood of cybersecurity or privacy breaches compared to receiving data through an official channel (box 2.3). Some of these tools, such as screen scraping, require access to a consumer's login details to facilitate data collection, providing the third party with unfettered access to the entirety of a consumer's account – not just the data of interest – potentially on an ongoing basis (Treasury 2023c, p. 6). Users often have limited awareness and control over what is or is not accessed, and how data is collected, handled, and disclosed which can increase vulnerability to fraud and scams (OAIC 2023c, p. 1; Treasury 2023c, p. 7). The Commonwealth Bank of Australia found that customers that use screen scraping are at least twice as likely to experience fraud on their accounts (Eyers 2020). Moreover, they also surrender important safeguards: under the ePayments Code, a bank need not reimburse losses if the customer has shared their passcode (ASIC 2022, p. 16).

Box 2.3 – What to do with screen scraping?

The Australian Government has sought advice from Treasury on how to progress 'a full and formal ban of screen scraping' (Jones 2024). This follows a consultation process in 2023 that sought feedback on banning the practice in sectors where the CDR provides a viable alternative (Treasury 2023c). Both the ACCC and the OIAC supported the proposal, noting the 'significant privacy and security risks' that screen scraping can pose for individuals (ACCC 2023; OAIC 2023c). However, industry groups warned that an outright or premature ban could strand tools that rely on the technology, shut out small lenders, and reduce service reliability where it functions as a fallback option (AFIA 2023, p. 2; FDATA 2023, p. 11; Fintech Australia 2023, p. 21).

The Productivity Commission (PC) considers that a phased approach to banning screen scraping would reduce the risk of major disruptions and unintended consequences by only applying the ban to a sector once an officially, secure and reliable alternative is widely available. In the interim, services could be required to clearly disclose their use of screen scraping to their customers so they are aware of the risks.

Alternative tools can also create significant security and operational risks for the data holder – undermining business fraud protection controls and making it more difficult to detect and identify the source of a data breach (ABA 2023, p. 6). Because consumers often re-use passwords across different services and service

providers, the compromise of login credentials held by a screen scraping service could facilitate multiple simultaneous data breaches (ABA 2023, p. 6).

Duplication and waste

Individuals and businesses that cannot access data directly may find it easier to re-collect or regenerate data (box 2.4). This results in duplication and waste, and at times can actively lead to consumer harm.

To illustrate, take the example of an individual who is unable to transfer their existing medical data to a new provider and as a result must redo their X-rays. This re-collection is costly – the consumer pays to have another set of often invasive or inconvenient scans, resulting in health risks and delays to their medical diagnosis and treatment.

Box 2.4 – Examples of the re-collection of data that already exists

Re-collecting data happens every day – individuals book a new doctor's appointment to swap their paper prescription to an e-script, pathology tests are duplicated when data cannot be moved to a new provider, and data that is not machine-readable is rekeyed manually. Reducing redundant data collection, storage and maintenance would deliver significant benefits.

- Electronic medical record systems rolled out across all public hospitals would save \$355 million through reduced duplication of pathology tests and imaging (PC 2024a, p. 2).
- The processing of a traditional invoice requires substantial manual entry. The adoption of the Peppol e-invoicing system can reduce processing costs by almost 70% (ATO 2024).
- A paper prescription cannot be converted to an electronic one, and vice-versa, without an individual booking a new consultation with their doctor to request it (RACGP 2021).
- A UK study found that enabling SMEs to give lenders direct access to their tax data via an API could reduce loan application times by half and increase loan offers by 20% to 40% (CFIT 2024, pp. 16–17).

Data access is unlikely to improve on its own

Data holders don't always like to share ...

Data has become a core asset in modern business models - it is a critical input for decision-making, diagnostics and operations management, but is also often a product in its own right and source of competitive advantage (CCAF 2024, p. 51; OECD 2022a, p. 5; O'Mahoney et al. 2022, p. 9). This creates strong incentives for firms to maintain a tight grip on the customer data they control to protect the value they can generate from it (Castro and Steinberg 2017; Deloitte 2023, p. 16).

For some, exclusive control of customer data provides a direct revenue stream. Providers can on-sell or licence the data they collect to third parties – such as car manufacturers who on-sell telematics data – or charge users to access data and analytics from their devices – such as video captured by smart cameras (CHOICE 2024). For other providers, control of the data they hold can help them to shore up market share (OECD 2022a, pp. 5–6). Firms can both *lock their customers in* by making it difficult to transfer data to another service or *keep their competitors out*, by preventing other products or services from integrating with their own (Gulati-Gilbert and Seamans 2023; OECD 2022a, p. 27, 2024b).

Providing data access can also be costly and challenging.

- Supporting secure data access often requires significant upfront investment and ongoing costs, especially for firms with fragmented or outdated back-end systems (ABA 2020a, p. 10; Accenture 2024a, p. 24; Treasury 2021, p. 7, 2023b, pp. 10–12).
- Collecting and holding larger volumes of data may increase cybersecurity vulnerabilities. Cyberattacks can result in major disruptions, large fines and reputational harm (Gao et al. 2025, p. 1; Liu and Babar 2024, pp. 11–17). Mitigating this risk requires strong managerial oversight and long-term investment in cyber defences (Liu and Babar 2024, p. 17).
- It can increase the regulatory requirements that providers need to comply with. The Australian Institute of Company Directors (sub. 8, p. 15) submitted that the ‘maze’ of data handling obligations act as a handbrake to more dynamic utilisation of data and create specific risks.

Data holders also face a ‘chicken and egg’ coordination dilemma (Fernandez et al. 2020, p. 1; Krämer et al. 2020, p. 76). A provider that opens up consumer data may bear the costs without seeing immediate benefits – especially if there isn’t an existing ecosystem of third-party services that can enable consumers to put the data to use. Meanwhile, third parties are unlikely to invest in developing their own services unless they can rely on broad, ongoing access to consumer data in a sector.

... and individuals and businesses lack awareness and are easily discouraged

Despite its benefits, data access is rarely front of mind for consumers. Most people are unaware of what data is collected about them and by whom, and don’t consider what data they can or can’t access from a product or service before making a purchase (ACCC 2024b, p. 6; EIG 2023, p. 23). Individuals can also face difficulties in judging the relative trustworthiness, safety and reliability of data access tools and services (OECD 2023a). A survey found that while Australians are heavy users of digital technology, only 12% of consumers have a clear understanding of how their personal information is collected and shared (CPRC 2020, p. 14).

At the same time, consumers increasingly expect their digital interactions to be seamless and thus are easily put-off when accessing or sharing their data isn’t straightforward (Deloitte 2024a, p. 25). Frollo, a financial management app and Accredited Data Recipient under the CDR notes that 5% to 65% of users do not make it through the consent authorisation step (Frollo 2024, p. 7). This drop off has been attributed to technical and user design issues with the CDR’s consent process (Frollo 2024, p. 7; Skript 2024, p. 7; WeMoney 2024, p. 6).

Existing data access policies do not provide a pathway to scale up data access across the economy

The Australian Government continues to invest in policies that are intended to support data access. The CDR, MHR system and the Motor Vehicle Service and Repair Information Sharing Scheme⁹ are improving data access within their respective domains, but they remain siloed and disconnected, limiting the potential to scale up data access across the broader economy.

The CDR was established as an economy-wide scheme vesting the Treasurer with powers to designate sectors and the classes of data that will be covered. It was designed to allow operational rules (e.g. eligibility criteria) and aspects of the data sharing approach to be tailored to different sectors (ACCC 2025b; Treasury 2025a). However, core parts of the CDR’s architecture apply to any designated sector. This

⁹ The Motor Vehicle Service and Repair Information Sharing Scheme mandates that manufacturers share information that is required to service and repair vehicles with repairers and registered training organisations at a fair market price (ACCC 2025a; Treasury 2025b).

includes its accreditation model, bespoke privacy safeguards and key technical requirements (e.g. standards specifying how APIs must be built). Together the set-up costs of these features impose a high bar for bringing new sectors into the scheme.

Taking stock of this, the Australian Government has paused further expansion of the CDR and announced a ‘reset’ that will focus narrowly on addressing issues that are driving costs and limiting take-up in already-designated sectors (Jones 2024b, 2025). Although other sectors have been designated (i.e. telecommunications) or considered for designation (e.g. superannuation), there are currently no plans to roll the CDR out beyond non-bank lending (Australian Government 2022; Jones 2024b; Treasury 2022a, p. 2).

New regulatory pathways to expand data access

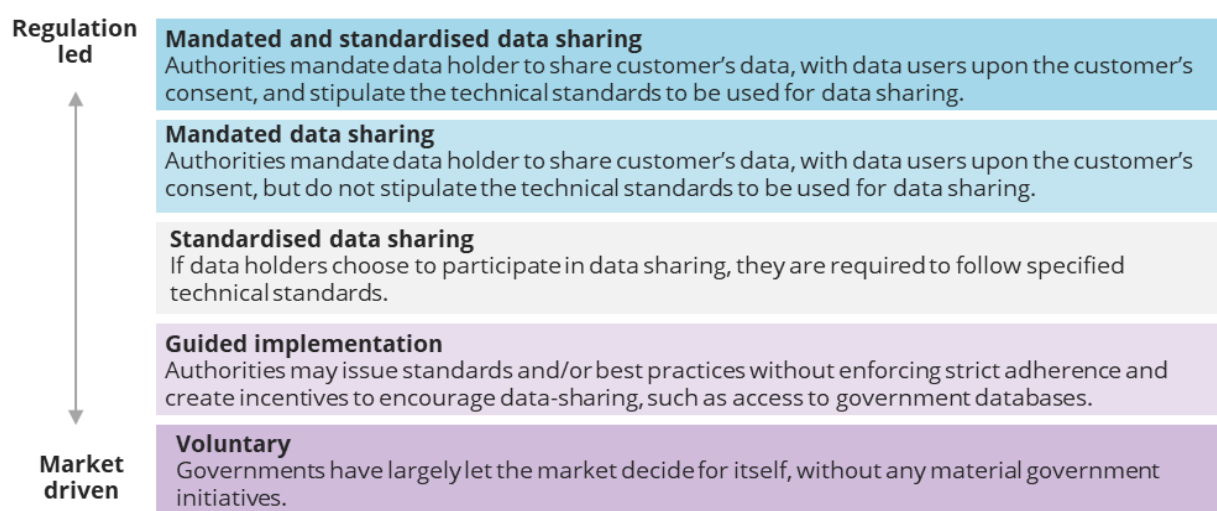
Government can provide the impetus to expand data access ...

Governments around the world are taking steps to give individuals and businesses better access to data that relates to them. Since the United Kingdom (UK) introduced ‘open banking’ in 2016 to give customers access to their transaction data, 60 jurisdictions have followed suit, with 16 extending their data-sharing regimes to cover a range of financial services such as insurance, mortgages, and pensions (CCAF 2024, p. 40).

Australia has been among the countries leading the way, and the CDR has become a reference model for other jurisdictions (DBT 2024, p. 13; OECD 2023b). Both the European Union’s (EU’s) *Data Act* and the UK’s *Data (Use and Access) Bill 2025* signal an international trajectory towards data access regimes that can span across the economy (DBT 2024, p. 8; EC 2025a).

Regulatory approaches to data access vary widely, ranging from industry-led codes of conduct to prescriptive models with government-defined rules and technical standards (figure 2.2). There is no ‘best’ model. Rather, the choice depends on each country’s legal frameworks, institutional capacity, and market conditions (CCAF 2024). However, valuable lessons have emerged about how governments can maximise the benefits of data sharing – such as improved competition and innovation – while avoiding excessive compliance costs for data holders.

Figure 2.2 – Governance approaches to data access



Source: CCAF (2024, pp. 26–27).

... but broad mandates can impose large economic costs

Mandatory data-sharing obligations have often been essential to kickstart progress – especially in sectors where increasing competition is the primary objective. The Global State of Open Banking report found that mandatory requirements were essential to initiate data access in the banking sector (CCAF 2024, pp. 41, 49). In contrast, purely voluntary approaches have generally failed to gain traction, largely due to the limited cooperation of established market players with little incentive to share data (CCAF 2024, pp. 41, 49). However, sectors with different competitive dynamics may not require the same level of regulatory intervention. This highlights the importance of designing data access schemes that have flexibility to account for the particular structural characteristics of different sectors across the economy.

Being too prescriptive can undermine the incentives for data holders to participate and act as a handbrake on innovation (CIPL 2024, p. 10). The EU has taken the most expansive approach to regulation, combining broad economy-wide rights covering personal data (under the EU's *General Data Protection Regulation (GDPR)*), connected devices (EU's *Data Act*), and digital platforms (EU's *Digital Markets Act*) with sector-specific schemes for payments, energy, and vehicle maintenance data (EC 2024, 2025a; Krämer et al. 2020, p. 18). This approach has had positive spillover effects into other jurisdictions, with some firms that operate in the EU opting to provide the same data access capabilities to their customers in non-EU countries (CIPL 2024, p. 6). But it has imposed material costs for data holders (CIPL 2024, p. 19). For example, research by the National Bureau of Economic Research found that the introduction of GDPR in 2018 led to the exit of roughly one-third of apps from the Google Play Store, and a 50% drop in new app entries in the quarters following implementation (Janssen et al. 2022, p. 36). While the GDPR's cross-sector design aimed to create a universal standard for data access, its broad rules have limited its practical usefulness (Exposito-Rosso et al. 2022, p. 22).

Governments can play a critical role setting up an overarching framework for data access, but they do not need to design and control every aspect of its implementation. Moreover, a one-size-fits-all approach is unlikely to deliver intended outcomes across the board – different sectors have varying capabilities, types of data, and access needs. The next section lays out such an approach.

Lower-cost and more flexible regulatory pathways are needed to expand data access

Enabling individuals and businesses to access, transfer and bundle data about themselves can drive the creation of more personalised and effective products and services and help power productivity in the digital economy (Deloitte 2024a, p. 15; O'Mahoney et al. 2022, p. 9).

A one size fits all approach to data access is impractical. New lower-cost and flexible pathways are needed that will help to improve data access by allowing the obligations on data holders and the functions that governments perform, to vary according to the structural characteristics and digital maturity of different sectors in the economy.

These pathways will create a tiered 'data access' approach that, following a thorough consultation and vetting process, could be methodically used to expand data access starting with those sectors where the benefits of sharing data clearly outweigh the costs, and the costs are relatively low. This could include where new technology, international regulation or domestic developments show that there are clear net benefits to Australia. We provide three examples below that we consider meet this threshold: agricultural machinery and equipment data, supermarket loyalty data, and access to information for renters.

The pathways we envision will not be blindly or quickly imposed on the economy – rather they are intended to 'meet sectors where they are' and build from there. In a similar manner, the UK is taking a

sector-by-sector approach to implement its *Data (Access and Use) Bill*. We are interested in hearing from participants about their views on implementation approaches and timeframes.



Draft recommendation 2.1

Establish lower-cost and more flexible regulatory pathways to expand basic data access for individuals and businesses

The Australian Government should support new pathways to allow individuals and businesses to access and share data that relates to them. These regulatory pathways will differ by sector recognising that the benefits (and the implementation costs) from data access and sharing are different by sector. This could include approaches such as:

- **industry-led data access codes** that support basic use cases by enabling consumers to export relatively non-sensitive data on a periodic (snapshot) basis
- **standardised data transfers** with government helping to formalise minimum technical standards to support use cases requiring high-frequency data transfers and interoperability.

These pathways should be developed alongside efforts that are already underway to improve the Consumer Data Right (which will continue to provide for use cases that warrant its additional safeguards and technical infrastructure) and the My Health Record system.

The new pathways should begin in sectors where better data access could generate large benefits for relatively low cost; and there is clear value to consumers. Potential examples include:

- enabling farmers to combine real-time data feeds from their machinery and equipment to optimise their operations and easily switch between different manufacturers
- giving tenants on-demand access to their rental ledgers which they can share to prove on-time payments to new landlords or lenders
- allowing retail loyalty card holders to export an itemised copy of their purchase history to budgeting and price comparison tools that can analyse spending and suggest cheaper alternatives.

The scope of the data access pathways should expand over time based on industry and consumer consultation, where new technology, overseas experience or domestic developments show that there are clear net benefits to Australia.

Where should new access pathways focus?

Data regulation needs the flexibility to recognise that the specific types of data that will be most valuable to individuals and businesses and the form of access needed to enable their use will vary from use case to use case. Similarly, it should recognise that the costs of providing access can vary significantly depending on what data holders need to share and how. To deliver their intended net benefits, the scope of the new data access pathways must balance the desire to improve data sharing against the potential to undermine incentives to collect, store and add value to data, recognising that any approach to access that leads to less data being productively used will lower, not raise, productivity.

What data is relevant?

The scope and types of data available to individuals and businesses need to be sufficient to allow it to be put to use. If the scope of data access is too limited there will be no incentive or ability for intermediaries and third parties to use it to provide useful and innovative services.

While the exact data that is accessible will vary on a case-by-case basis, it will need to meet three criteria.

- i. It is identified with the consumer or business.
- ii. It is held or controlled in digital form by the providers of the goods and services they use.
- iii. It is collected or created through their interactions with them.

For example, this could include data that individuals or businesses have either provided themselves (e.g. name, address, date of birth, revenue), or has been obtained (e.g. purchased from a third party) or derived about them (e.g. salary). It could also include data that has been captured or generated by the products and services they use (e.g. click-streams and energy metering data).

‘Value-added’ or inferred data that has been produced or materially enhanced via proprietary algorithms or analytics (e.g. risk scores or ad-profiles) should be excluded. So should any data that cannot be ‘reasonably’ identified with a person or business (e.g. aggregated or de-identified data). This broadly aligns with the existing scope of the CDR and similar international data access regimes (table 2.2).

Table 2.2 – Data types that are in and out

Data type	Example	In scope	In CDR
Profile / account data	- Name, address, Australian Business Number - Purchase history, fees, SOPs	✓	✓
Other personal information	Income, age, gender, household composition	✓	✓
Commercial / operational information	Revenue, salary costs, production volumes	✓	X
Transaction / activity data	Bank transactions, metering data, Point of Sale data, click-streams	✓	✓
Device / equipment data	Solar inverter output, telematics and sensor data	✓	✓
Inferred data	Credit risk assessment, risk appetite, driver safety profile, retention expectancy	X	X
De-identified data	Aggregated datasets, generalised data (i.e. full address is generalised to region)	X	X
Product data	Product features like interest rates and fees and technical specifications (e.g. battery capacity)	? ^a	✓

a. In some sectors or industries only.

Who could be asked to provide access to data?

The new access pathways will focus on data relating to products and services that are provided to individuals and businesses. Often this data is collected by the private sector. This could include data held or controlled by retailers, manufacturers, service providers and digital platforms. Access should only apply to

data holders that are ‘custodians’ of the data – it would not apply to cloud services (e.g. Amazon Web Services) that store the data on behalf of product and service providers.

There may also be situations where the new pathways could be applied to services that are delivered or funded by government. Allied health data might be one example, although this would need to be assessed on a case-by-case basis, in consultation with the relevant allied health professionals and organisations, being careful to avoid duplicating data use cases covered by existing government data initiatives, like MHR. The parties collecting the data may be private businesses (e.g. a private dental practice) or a government organisation (e.g. a public dental clinic).

The new regulatory pathways would not apply to all data holders all at once. Instead sectors could be incrementally designated to them based on a readiness review assessment (discussed in more detail below).

Making the most of what’s available – permissions, access mechanisms and standards

Having ‘access’ to data is insufficient – individuals and businesses must also be able to seamlessly put it to use (Deloitte 2024a, p. 25; Exposito-Rosso et al. 2022, pp. 21–26). At a minimum, this means they need to be able to obtain a digital copy of the required data (as opposed to, for example, having to manually take a photo of a paper bill and email it on to a service provider), which they can share with whoever they choose.

But much of the value that individuals and businesses can gain from the data that relates to them relies on their ability to *transfer (or switch) it from one provider to another (data portability)* or to *link the related products and services they use together (interoperability)* (Gulati-Gilbert and Seamans 2023). Fundamentally, data portability and interoperability reduce the frictions that put off individuals and businesses from trying new products and getting the most out of them (OECD 2021a).

While data portability and interoperability are closely related, interoperability necessitates the use of more advanced access mechanisms.

- Transferring data between services requires a point in time export in a structured and transparent machine-readable format (i.e. the data fields, what they mean, and the values they can take are clearly defined and/or conform to common standard) (Krämer et al. 2020, pp. 37–39).
- Interoperability requires two systems to be able to communicate with each other on an ongoing basis and often continuously. This relies on common technical specifications which may be formal protocols (e.g. Simple Mail Transfer Protocol for email traffic) or APIs that are either based on open standards or defined by one provider for others to use (Gulati-Gilbert and Seamans 2023; OECD 2021b, p. 13). For example, businesses who use Square’s Point of Sale (PoS) terminals and Xero can link their accounts to enable sales transactions to be auto-posted daily to their general ledger (Square 2022).

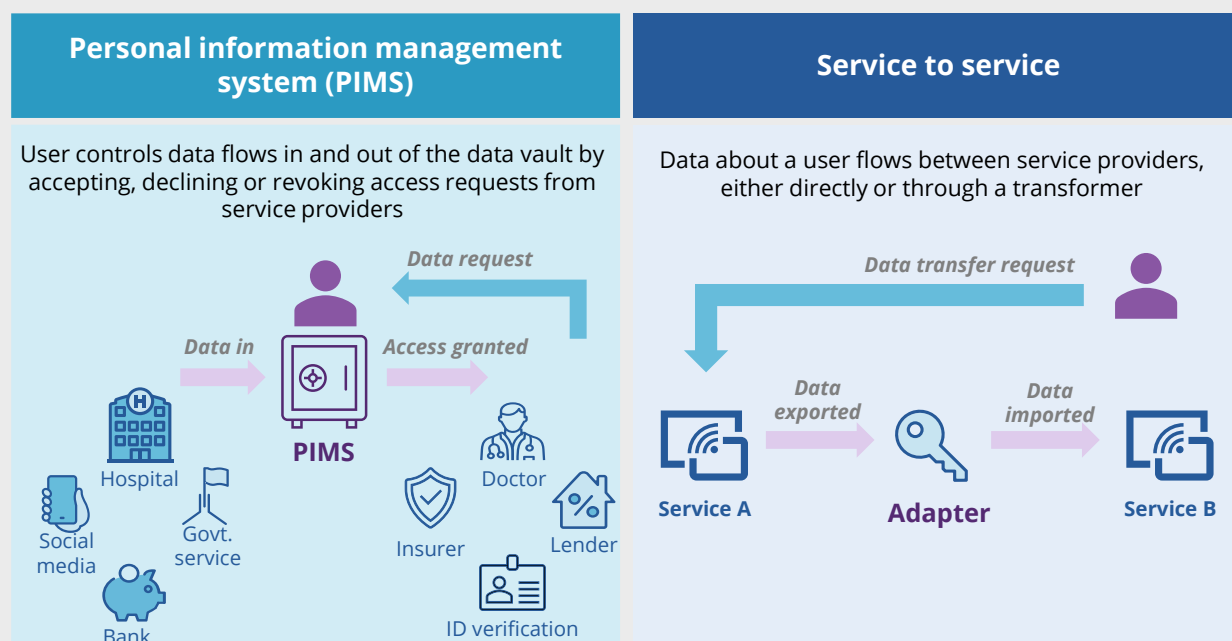
As well as being able to view and transfer data, some high value use cases require altering data at its source (write access). Write access can enable third parties to initiate actions or updates, such as making payments, transferring funds or updating personal information (CCAF 2024, p. 29). According to the Global state of open banking report (2024, p. 51), 55 jurisdictions have implemented ‘write-access’ within their open banking regimes to enable third parties to initiate transactions. This capability has been legislated for use in the CDR regime but is yet to be implemented (Jones 2024a).

Specialised data intermediaries can help make all this possible: they can develop common standards, build open APIs, verify identity and consent, and embed security and assurance protocols (DTI 2024a, p. 2; WEF 2022, p. 9). By doing so they can reduce the costs that data holders would otherwise incur and help establish trust between the parties who are sharing the data (box 2.5).

Box 2.5 – The role of data intermediaries

Data intermediary is an umbrella term for third-party entities that facilitate data sharing and help manage the relationships between individuals, businesses and data holders. Intermediaries come in many forms and can assume a range of roles (which may include processing, aggregating and enhancing data) that are better or less suited to different use cases (WEF 2022, pp. 9–10). Two examples are *service-to-service* models and Personal Information Management Systems (PIMs).

Service-to-service models – such as the Data Transfer Initiative - act like transformers, converting proprietary formats into common ones so that users of platforms such as Google, Meta, Microsoft, and Apple can directly port their photos, files, playlists etc from one service to another (DTI 2018, pp. 5–6). In contrast, PIMs, let users collate data about them that is siloed across many providers into a secure store that they can grant or revoke access to (CDEI 2022, p. 20). They can also then help individuals to use the data by presenting it user-friendly dashboards, enhancing its quality or enriching it with analytics (OECD 2019, p. 36). For example, Apple’s HealthKit app allows iPhone users to analyse trends and generate insights that can be shared with health-care providers (Apple Developer nd).



Right-sizing data access requirements to minimise regulatory burden

Efforts to expand data access will only be successful if they minimise the regulatory burden for data holders and potential users (e.g. intermediaries and third-party providers). They should focus on making things as easy and simple as possible for individuals and businesses to make use of the data that relates to them.

There are many different approaches and technologies that can be used to enable data access. For some use cases, simple access mechanisms that allow data to be downloaded or exported on a periodic basis will do the job. For example, Bill Hero is an Australian energy comparison and switching service which helps users find lower cost plans by uploading or forwarding PDF copies of their bills (Bill Hero 2024). Other use cases, such as those involving connected ‘smart’ devices, will require technical solutions and access

mechanisms that allow data to be transferred ‘continuously’. Recognising that these ‘continuous’ use cases are becoming more common, both the UK’s *Data (Use and Access) Act 2025* and the EU’s *Data Act* include provisions that obligate some data holders to allow users to transfer data from their devices in ‘real time’ (European Parliament 2023b; UK Parliament 2025).

The way in which use cases are ‘solved’ (i.e. via a technical solution imposed by industry, government or an independent data standards board) needs to take account of the different capabilities of data holders, and the costs (and who bears them, and how) of implementing preferred solutions. Prescriptive requirements that mandate specific technologies may lock in inferior standards and prevent the emergence of superior solutions (CIPL 2024, p. 16).

New access pathways should keep blanket requirements to a minimum, and to the extent possible, remain technology neutral. But at the same time, they will need to facilitate the establishment of appropriate data access mechanisms that can support a broad range of ‘reasonable’ uses on a case-by-case basis for different sectors and data products.

What might new access pathways look like?

The introduction of new access pathways could provide a simple, ‘graduated’ ladder to enable data access that will support high value use cases across different sectors. Rather than trying to fit all sectors under a single scheme, the pathways could allow the regulatory obligations on data holders to vary according to the sensitivity of the data they hold and complexity of its potential use cases. To do this, the pathways could differ in terms of the form/s of access they support (e.g. periodic downloads vs continuous transfers); the technical and performance specifications they require and, the security controls and safeguards they enforce (figure 2.3).

An *industry-led* pathway, and a *standardised data transfers* pathway are discussed below to illustrate how the new pathways could be designed and the types of use cases they would support.

Industry-led basic data exports

This pathway could enable individuals and businesses to access relatively non-sensitive data that relates to them on a periodic, or ad-hoc, basis. Specifically, **data users** could expect access to point-in-time, machine-readable data exports via ‘single pull’ requests. To get the pathway up and running, **data holders** would require an agreed definition of the core data fields that they will need to make available, and the basic common technical specifications (e.g. the file types and data standards) they would need to support. Data holders would also be responsible for managing their own security controls (i.e. this pathway would not enforce an accreditation model).

The ‘rules’ of the pathway could be set out and agreed on in sector-specific data access codes and overseen and monitored by an appropriate oversight body. The Australian Government could play a role to convene industry representatives to develop data access codes for their sectors. It could also periodically review their uptake and assess their effectiveness at improving access conditions.

Standardised data transfers

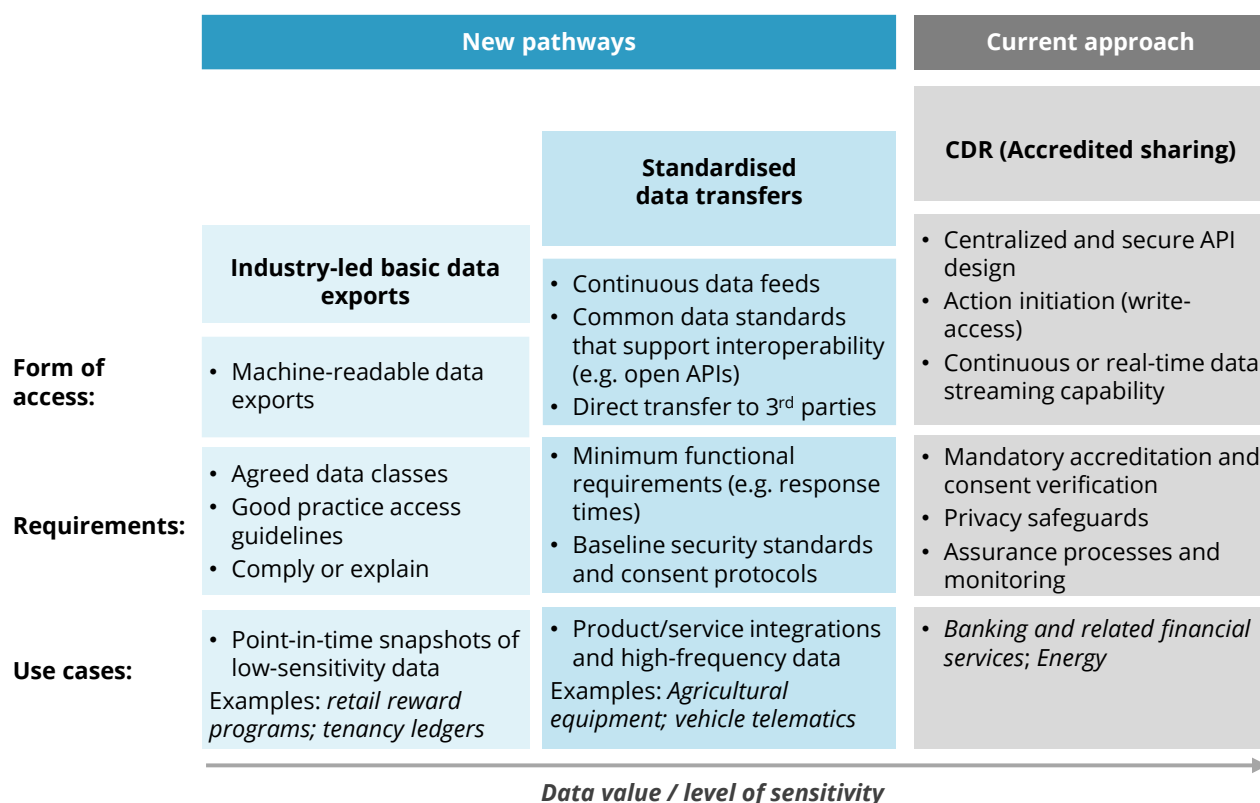
This pathway could move beyond ad-hoc data snapshots to enable individuals and businesses to directly transfer data to third-parties and support use cases involving high-frequency data and product/service integrations (e.g. ‘charge my car when my solar panels are generating power’).

Data users could expect continuous data feeds and interoperability across different applications. To get the pathway up and running, **data holders** would need to support an agreed set of common data standards, API

specifications and basic reliability thresholds (e.g. response times). Data holders and third-party providers would also need to implement minimum security controls, such as open authentication consent protocols, encryption, audit logging and mandatory incident reporting.

The Australian Government could act as a technical steward. This could include working with industry to formalise the minimum technical requirements and standards that providers will need to implement and managing updates as needed. It could also conduct basic performance testing and issue penalties for serious breaches.

Figure 2.3 – Potential new data access pathways



These two proposed pathways could eventually operate alongside the CDR and MHR data sharing initiatives, both of which are undergoing reform (box 2.6). The CDR will continue to operate as a pathway for sectors and/or use cases that require the access functionality, reliability and security capability that its core architecture and digital infrastructure has been designed to provide (namely its accreditation model, core rules and technical standards and enforcement tools). This includes use cases that involve third parties issuing authorised instructions on behalf of services users (such as initiating payments or switching providers).

Box 2.6 – Continue to course correct existing data sharing initiatives

The development of new data sharing pathways should occur in tandem with ongoing efforts to improve the Australian Government's Consumer Data Right (CDR) and My Health Record (MHR) initiatives. Both programs have been subject to review processes, and implementing their findings will help to deliver unrealised benefits and may encourage wider adoption of data access tools and services as they become more available in other sectors.

- MHR was designed as a secure platform to let individuals easily access and share their health information across providers. Yet despite more than \$2 billion in investment, only about 2% of uploaded documents have been viewed by another provider (PC 2024a, pp. 2, 24). To fix the system's incomplete records and patchy coverage the Australian Government has passed the *Modernising My Health Record (Sharing by Default) Act 2025* to compel certain providers (e.g. pathology and diagnostic-imaging providers) to upload test results by default, unless an exemption applies (DHAC 2025). It has also allocated \$2 million to increase the number of allied-health software platforms that are compatible with MHR and electronic prescribing (ADHA 2025; DHDA 2025a).
- The Australian Government is also progressing a 'reset' of the CDR, which it announced in August 2024 to reduce compliance costs and increase uptake. This includes consideration of rule changes that will streamline how business consumers consent to data sharing, reduce the period of data that must be shared from 7 to 2 years and remove requirements on sharing 'niche' product data, while also expanding the CDR to non-bank lenders (Jones 2024b, 2025). The implementation of these changes could help reduce the cost of bringing in adjacent sectors in the future (e.g. superannuation).

The pathways in action

The PC has identified three use cases that we think could have large benefits for Australian individuals and businesses.

1. Agricultural machinery and equipment data

Much of the machinery and equipment that farmers now use has extensive data collection capabilities which can capture both machinery (e.g. speed and temperature) and production data (e.g. crop yields and soil quality) (ACCC 2021, p. vi). As this data accumulates over time it can be used by farmers to help them better manage their operations and respond to seasonal variability.

But, because the data captured by different equipment manufacturers is often incompatible, farmers can struggle to make the best use of it – resorting to using multiple dashboards or paying for additional unofficial tools to stitch it together (ACCC 2021, p. 53; Knights 2023; Newman 2022). The 2024 Australian Agritech Association sector report highlights that a lack of common data standards to enable interoperability is holding back the adoption of agritech solutions that can improve farm productivity and sustainability (AusAgritech 2025, pp. 11, 44). The Australian Competition and Consumer Commission (ACCC) has also found that the inability to transfer data between different brands of machinery can result in farmers being 'locked in' to particular brands (ACCC 2021, p. 50).

In 2020, the National Farmers' Federation introduced a voluntary Australian Farm Data Code to help support trusted data sharing and the adoption of digital technology (box 2.7) (Dale and Heath 2023; NFF 2023b). The application of the *standardised data transfer* pathway could bolster the Code by obliging manufacturers to adhere to existing ISO-based data standards and provide data via secure open APIs.

Box 2.7 – The Australian Farm Data Code

Developed by the National Farmers' Federation with support from the Australian Government and input from farmers, researchers, and tech providers, the voluntary Australian Farm Data Code aims to promote transparency, trust, and responsible data practices in agriculture by:

- increasing awareness and understanding of the ways in which providers are collecting, using and sharing their farm data
- preserving farmers' ability to determine who can access their data, and allow them to access and retrieve their individual data
- providing a framework to compare providers and inform negotiations about data policies
- bringing about improvements to industry-wide data practices over time.

By helping farmers understand how their data is collected, used, and shared, the code empowers them to make informed decisions, compare service providers, and supports greater digital adoption and consistent data governance across the sector.

Source: National Farmers' Federation (2023a).

2. Real estate tenancy data

To get proof of rental payments, residential tenants often need to request a copy from their property manager, which can take up to seven days in some jurisdictions to be fulfilled (NSW Government 2024). Some property-management portals allow users to download a PDF copy or extract a CSV file (OurProperty 2025). But as there is no standard format that landlords or agents need to use, the layout and information included in rental ledgers varies, which can make them difficult for tenants to understand and reconcile (Tenants' Union of NSW 2025, p. 2).

Designating tenancy data to the *industry-led* pathway could oblige property managers to enable tenants to download their rental ledgers on-demand in an easy-to-read and standardised file format. This would enable renters to easily attach their payment history to new-rental applications and allow banks and fintechs to quickly verify rent payments for loan applications.

3. Retail loyalty rewards data in digital form

Loyalty programs - such as Woolworths Rewards - collect large volumes of detailed data about customers' shopping habits (CHOICE 2021). 'Brick and mortar' retailers are increasingly turning to third-party 'smart receipt delivery platforms' to provide their customers with digital receipts. For example, retailers such as Chemist Warehouse and Harris Farm use *Slyp* to provide their customers with digital receipts via text message or directly to their banking app (Jerez 2021; Slyp 2025). These platforms enable retailers to connect data from their PoS and e-commerce systems with loyalty programs that are linked to customer payment cards to generate 'hyper-personalised customer engagement' and purchasing insights (Slyp 2025).

Digital receipts can allow customers to retain a record of their purchases. But because they are typically provided in an unstructured PDF or other 'read-only' format, they cannot readily use the data themselves to compare prices or track their spend. Enabling customers to easily export the transaction data from their digital receipts and loyalty accounts could allow them to share it with third-party apps that offer budgeting, habit tracking, tax reporting, and other personalised tools.



Information request 2.1

The PC is seeking feedback on how to introduce lower-cost and more flexible data access pathways for a broad range of use cases. In line with draft recommendation 2.1, we are also seeking feedback on the sectors and use cases where the new pathways could most valuably enhance data access in the short term. We note that the banking and energy sectors are already covered by the Consumer Data Right.

- **What types of data should be covered by the pathways?** Are there any issues with the data types proposed in *table 2.2* that should be considered?
- **How should data be made available under each of the pathways?** Could the scope and requirements outlined for the proposed *industry-led basic data exports* and *standardised data transfers* pathways effectively support a broad range of use cases?
- **Where should data access be prioritised in the economy?**
 - Which sectors or data holders already enable individuals or businesses to access data overseas due to local laws, but are not meeting comparable standards of sharing in Australia?
 - Which sectors or data holders in the economy have data that could be accessed in a useful, digital format to support high value use cases at low cost?
 - Which sectors or data holders are already trading data about individuals or businesses with third parties, so that access to that data could be achieved at a low incremental cost?

A methodical approach to bringing new sectors online

The proposed data sharing pathways are intended to ‘meet sectors where they are’. Rather than imposing onerous requirements on data holders or a rapid overhauling of existing technology, they will operate to formalise existing best practice and provide guidance for more basic operators on how to uplift their data management systems. The longer-term aim would be to create more consistent and useable access to data for individuals and businesses across the economy.

A review process could be established to identify and assess the ‘readiness’ of individual sectors to be designated to a pathway. The readiness review process should be led by a body with the appropriate expertise and capability. The ACCC or the Data Standards Body are potential candidates given their existing roles and accumulated experience under the CDR regime.

The readiness review would assess prevailing data sharing practices and constraints on high value use cases, as well as market dynamics and the technological capacity of data holders (*table 2.3*). The review could potentially be guided by the *Voluntary Data Classification Framework* that is being developed by the Department of Home Affairs and CSIRO’s Data61. This framework is intended to provide a consistent way to assess and classify the potential value and sensitivity of the data that different industries hold to inform the application of proportionate security controls and governance approaches (Department of Home Affairs 2025).

A readiness review should, in the first instance, identify opportunities to enhance data access where there are large potential benefits and/or low marginal compliance costs. This could include sectors with known high-value use cases or where providers have already enabled data access for their customers/service users overseas (e.g. the EU’s *Data Act* will require smart device manufacturers to engineer their products so that users can transfer device data in real-time to third parties of their choosing) (EC 2025a). Rather than being designated, sectors could also potentially have the option to voluntarily opt-in to an access pathway.

The PC is seeking views on how sectors could be identified to undergo the readiness review.

Table 2.3 – Considerations for assessing the data access readiness of sectors

Dimension	Types of considerations
Prevailing data practices	What customer level data do providers already release, and how sensitive is it? Are they subject to similar data access obligations in other jurisdictions?
Demand/Use cases	What are the potential use cases for the data? Can it enable the use of related services? Are users resorting to work arounds today? Do overseas examples show strong uptake when comparable data is shared?
Market structure	How are providers using the customer data they hold? Do they charge access fees or licence it to third parties? How competitive is the sector and does it exhibit network effects? How easily can consumers switch between providers?
Cost and technology maturity	What are the costs (and sunk investments) involved in collecting and sharing the data? Do common standards, APIs, cybersecurity practices and data intermediaries already exist in the sector?

The role of government in making data access worthwhile

The PC wants to hear from participants on the role government should play in the development of the pathways. For example, as discussed above, government could use its convening powers to bring together industry groups, and set up standards boards to act as technical stewards.

Experience abroad and in Australia has shown that governments can leverage the private sector to help with the heavy lifting in setting up and running data sharing schemes. For instance:

- trusted data intermediaries can help to reduce the need for governments to define technical rules and build its own systems and interfaces (CDEI 2022, p. 20; WEF 2022, p. 32)¹⁰
- industry-led initiatives such as the Road Infrastructure Management data sharing scheme and the Australian Farm Data Code demonstrate the capacity and willingness of sectors to develop and commit to sector specific data sharing codes (NFF 2023a; TCA 2025)
- in the UK, government-backed ‘Smart Data’ hackathons have crowd-sourced innovative use cases, accelerating the development of applications such as streamlining property transactions and mortgage applications (DTB 2025, pp. 20–21).

The legislative role of government – for example, using mandates as opposed to relying on voluntary action or market discipline – could be important when the incentives of data holders and potential users are not aligned (CCAF 2024, pp. 25–26). International experience suggests that reliance on regulatory mandates alone is unlikely to effectively engage data holders or promote an ecosystem of intermediaries and third-party providers who can put the available data to use (Deloitte 2023, p. 22).

To realise the full potential of data access, the pathways will need to provide ‘pull’ incentives alongside ‘push’ compliance obligations. Governments have several potential levers.

- **Reciprocity:** Obliging third parties to share data back to data holders (with customer consent) can prevent a one-way flow of value from incumbent data holders to new entrants or data ‘gatekeepers’ (Deloitte 2023, p. 22). An OECD (2023b, p. 28) survey found that Germany, Türkiye and Brazil allow for reciprocal data

¹⁰ The government of Flanders has partnered with Inrupt to roll-out its portal which allows citizens to access data across different agencies and use it to engage services and verify information about themselves with third parties (Inrupt 2022)

access between all parties involved in data sharing arrangements. Another option, as recommended by the 2022 Statutory Review of the CDR, is to make government datasets available so ‘consumers can share their data across a greater range of services’ (Treasury 2022b, p. 62).

- **Targeted tax measures:** Investment or accelerated depreciation could incentivise firms to upgrade legacy data system and/or build out necessary infrastructure.
- **Incubators and grants:** These can help to seed new use-cases and build awareness and momentum, as shown by the UK’s hackathon events (DTB 2025).
- **Fees and charges:** In some situations, fees and charges may be negotiated between data holders, data seekers and third parties. For example, the Motor Vehicle Service and Repair Information Sharing Scheme allows manufacturers to charge repairers a price that does not exceed ‘fair market value’ for access to diagnostic data (Treasury 2025b, p. 13).

The issue of trust and privacy will also be important, and these issues are covered in chapter 3 of this report.



Information request 2.2

The PC is seeking feedback on how the new data access pathways could be expanded over time in a methodical and predictable way, while enabling innovation. We are also interested in views around how the Australian Government can best support this process.

- What should the readiness review process look like?
 - How should sectors and data holders be identified to undergo the readiness review?
 - What criteria should be considered in the readiness review?
 - Which body – either new or existing – should do the assessment?
- How do we best engage data holders or promote an ecosystem of intermediaries and third-party providers?
 - Should data holders be able to apply fees and charges?
- What role should the Australian Government play in the development and coordination of the pathways, and supporting its success?
- What is a reasonable timeframe for designing and implementing data access pathways?

3. Supporting safe data access and use through outcomes-based privacy regulation

Summary

- * The safety of data access and use is key to realising productivity growth opportunities.
- * As one of the main tools for ensuring safe data access and use, the Privacy Act places obligations on regulated entities who collect, use and handle personal information. Well-designed privacy regulations should effectively deliver privacy outcomes for individuals, while minimising compliance costs for businesses.
- * While overall, the Privacy Act provides flexibility, some requirements focus too much on specific controls (that is, prescribing certain actions or procedures) rather than outcomes. This can contribute to excessive regulatory burden without improving outcomes for individuals.
 - The consent, notification and disclosure requirements in the Privacy Act can be overly burdensome and difficult to comply with for some regulated entities, raising compliance costs without providing the protections individuals expect.
 - Overreliance on these mechanisms, and privacy policies, can undermine the safety and privacy interests of individuals and contribute to 'consent fatigue'.
- * Some of the recommendations from the Privacy Act Review could increase regulatory burden with little if any additional benefit for individuals. In particular, the proposal to introduce a right to erasure should not be implemented.
- * The Australian Government should introduce an alternative compliance pathway to the Privacy Act that allows regulated entities the option to fulfil their privacy obligations by meeting outcomes, rather than controls-based rules. This would provide entities with greater flexibility, choice and scope to innovate. It could also reduce the burden on individuals while better protecting their privacy interests.
 - The Productivity Commission is seeking feedback on design and implementation issues, including how an alternative compliance pathway should be embedded in the Privacy Act.

The productivity benefits of data access and use can only be realised if there is trust that the party providing access to the data has the right to do so, trust that the system of access is safe and secure; and trust that the party accessing the data will handle the data safely.

Government policy-setting can help enable those benefits to be realised, while managing the risks of data use, and misuse – including through robust regulatory settings that encourage firms to handle data in a safe and secure manner and provide enforcement regimes with penalties for failure to do so.

Privacy regulation is one way that governments seek to achieve this balance (box 3.1). There is a risk, however, that poorly designed privacy regulations can create excessive compliance costs for business or fail to deliver privacy outcomes for individuals. This reform is about making sure Australia's privacy regime underpins trust and is sufficiently flexible so that it achieves privacy outcomes, without overly burdening regulated entities. In turn, a robust and effective privacy regime will facilitate data access and use, boosting innovation and productivity across the economy.

Box 3.1 – What is privacy?

Although most people have an intuitive understanding of what 'privacy' looks like in an everyday context, privacy is an 'elusive' concept and has no precise or universally accepted definition (ALRC 1983, p. 3; VLRC 2002, p. v). The Australian Law Reform Commission recognised four separate but related dimensions to privacy (2007, p. 114).

- **Information privacy** focuses on rules governing the collection and handling of personal data such as credit information, medical and government records. It is also known as data protection.
- **Bodily privacy** concerns the protection of people's physical selves against invasive procedures such as genetic tests, drug testing and cavity searches.
- **Privacy of communications** covers the security and privacy of mail, telephones, e-mail and other forms of communication.
- **Territorial privacy** is concerned with intrusions into domestic and other environments, such as the workplace or public space. This includes searches, video surveillance and ID checks.

In Australia, privacy regulation tends to focus on information privacy. This is also the dimension most relevant to data and digital technology – and therefore the focus of this reform.

In Australia, the main legislation for protecting information privacy is the *Privacy Act 1988* (Cth) (box 3.2). The Act seeks to promote and protect the information privacy of individuals by regulating how certain entities (including private firms and Australian Government agencies) handle personal information (OAIC 2023d).

The need to balance competing interests is reflected in one of the objects of the Privacy Act; to 'recognise that the protection of the privacy of individuals is balanced with the interests of entities in carrying out their functions or activities' (s. 2A(b)). This recognises that well-designed privacy laws can protect the privacy interests of individuals, while encouraging information access and minimising compliance costs – thus enabling innovation and productivity growth.

Box 3.2 – How does the Privacy Act work and who is covered?

The Privacy Act governs how personal information is handled. Under section 6 of the Act, personal information is defined as ‘information or an opinion about an individual, or an individual who is reasonably identifiable ... whether the information or opinion is true or not ... whether the information or opinion is recorded in a material form or not’ (s. 6).^a

Responsibilities under the Privacy Act apply to most organisations with an annual turnover greater than \$3 million and Australian Government agencies (OAIC 2023b). This includes: individuals, including sole traders; body corporates; a partnership; any other unincorporated association; and trusts (OAIC 2023b). Small business operators, registered political parties, state or territory authorities or a prescribed instrumentality of a state are exempt.

The Act places obligations on these entities when collecting and handling personal information, principally through the 13 Australian Privacy Principles (APPs) (OAIC 2023a). This includes:

- APP 1, which requires regulated entities to have a ‘clearly expressed and up-to-date’ privacy policy about the management of personal information
- APP 2, which requires regulated entities to provide individuals with the option of not identifying themselves or using a pseudonym when dealing with an APP entity
- APP 12, which requires regulated entities to provide the individual access to their personal information upon request, unless an exception applies.

a. There is a proposal to amend the definition of ‘personal information’ (table 3.1).

The Privacy Act in a changing data landscape

Since the introduction of the Privacy Act, technological innovation has dramatically changed the data landscape, with implications for privacy and the protection of personal information.

Thirty years ago, data for most people was primarily about details on paper ... With the mass digitisation of data, the capacity to collect data through everyday Internet activity and transactions, and through technologies such as sensors, cameras and mobile devices, means that what is ‘data’, and who can or should have a say in how it is collected, stored, transformed and used is no longer so simple. (PC 2017, p. 3)

Nowadays, it is increasingly common for businesses to collect or record personal information as part of a transaction. But consumers are often not fully aware of why their personal information is being collected, and how it may be used (ACCC 2024b). Some businesses, such as large digital platforms, have significant market and bargaining power, which can make these information asymmetries much more pronounced.

The Privacy Act has been subject to numerous reviews and reforms over the years. In 2019, the Australian Competition and Consumer Commission’s *Digital Platforms Inquiry Report* identified the need for the Privacy Act to adapt to the digital age. This resulted in the *Privacy Act Review*, which delivered its final report in 2023. Many privacy reforms in Australia have concentrated on expanding the rights of individuals, due to a view that individual agency is being eroded in the face of, for example, large digital platforms.

Some businesses find the Privacy Act to be overly burdensome

Overall, there are mixed views about how well the Privacy Act regime is working. As part of the Privacy Act Review consultation, some businesses or organisations covered by the Act reported that the Act and the Australian Privacy Principles (APPs) are operating well and are sufficiently flexible (ABA 2020b; Ai Group 2020; Insurance Council of Australia 2020).

But this view was far from universal. Some inquiry participants viewed the Act as overly burdensome, ineffective and the Productivity Commission's analysis demonstrates it can also be costly (box 3.3). As one participant submitted:

we recognise that the Australian Privacy Principles (APPs) are overly complex and challenging to interpret and comply with. The 13 APPs often overlap and interact in complex ways, making it difficult to understand which specific requirements apply in particular situations. Organisations must navigate multiple principles simultaneously, each with their own specific requirements and exceptions. (AICD, sub. 18, p. 14)

There was a shared view that the emphasis on consent, notification and disclosure is difficult to comply with, especially in the digital age. For example, in its submission to the Privacy Act Review, Adobe said:

The ongoing development of the digital economy, including through technological innovations such as the Internet of Things and robotics, will seriously challenge the ability of entities to comply with a prescriptive notice and consent model. (2020, p. 5)

Box 3.3 – The cost of protecting privacy^a

The Privacy Act affects about 277,000 firms in Australia. Among these firms, some may be data intensive and face stringent obligations. Others may hold little more than customer contact details and have limited obligations under privacy law. For these 277,000 firms there are three main costs to protecting privacy.

Opportunity costs are the potential benefits lost when firms prioritise privacy processes. Better utilising data could yield benefits on the order of a 0.5% rise in labour productivity^b (worth \$13 billion per year). Regulation can also have a stifling effect on firm entry, with fewer firms entering a market when rules are strict (see for instance Janssen et al. 2022). Reduced firm entry may reduce competition and innovation.

Ongoing privacy costs involve the ongoing legal and administrative requirements related to privacy. The PC heard that large organisations often have a central privacy team who conduct privacy impact assessments for new initiatives and then delegate implementation to other teams. The PC estimates that total direct privacy costs across the 10,000 affected firms with at least \$50 million in turnover in Australia are about \$2 billion per year. The PC was unable to quantify costs across the 267,000 affected firms with below \$50 million in turnover, but these costs may be significant given the number of firms affected.

Finally, there are **one-off and indirect costs**. Building privacy compliant systems (for example secure websites) may be expensive. Privacy regulation may also favour large firms, reducing competition. However, these costs are unlikely to be captured in survey evidence so have not been quantified.

a. More detailed information on data sources and assumptions is available in appendix B. **b.** Data use is determined by many factors, changes related only to privacy are unlikely to capture all potential benefits.

It also said ‘the “notice and consent” model is simply not sustainable’ and that the cumulative burden of these measures may ‘limit the ability of businesses to appropriately explain to their customers what information they are seeking to collect and how that information will be used’ (Adobe 2020, pp. 5, 9).

These views demonstrate that, while some regulated entities considered the Act to be sufficiently flexible, some aspects of the regulatory regime were considered to focus too much on controls rather than outcomes (box 3.4).

- The more controls-based APPs include those that specify the procedures for handling and disclosure of personal information, including consent and notification mechanisms (APPs 5 and 6).
- Some of the APPs are outcomes-based, such as the requirement about ensuring that the personal information the entity collects is accurate, up-to-date and complete (APP 10).

One complicating factor is that regulated entities sometimes expressed contradictory objectives – during consultation for the Privacy Act Review, several business participants called for both greater certainty (including through more prescriptive rules) and greater flexibility in the Privacy Act regime.

During consultation for this inquiry, the PC heard evidence of over-compliance – that is, businesses taking privacy measures beyond what is required by law. In some cases, this was a business decision. Some businesses operating internationally found it more cost-effective to comply with more stringent international regulations across all their markets, including in the Australian market. Others chose to implement additional privacy measures to manage the reputational risks that could result from breaches of privacy.

However, there was also evidence that businesses may have not fully comprehended what their regulatory obligations were, leading to unnecessary ‘compliance’ efforts – which impose additional costs but may not improve privacy outcomes for individuals. An example the PC was advised of was businesses unnecessarily seeking consent from individuals, leading to heightened costs for businesses and creating unnecessary hurdles for consumers. It is possible that businesses would benefit from further regulatory guidance or legal precedent to help them understand their regulatory obligations.

Some said that the Act does not adequately protect individuals

Some participants in this inquiry argued that the Privacy Act does not adequately protect the privacy interests of individuals. This is because the emphasis on controls, like consent and disclosure procedures, and privacy policies, do not guarantee positive privacy outcomes. Instead, they place the onus on the individual to manage and protect their own data.

Existing regulatory arrangements emphasise individualised harms. For instance, the dominant paradigm in the Privacy Act is of ‘privacy self-management’. The Act overwhelmingly focuses on the harms associated with collection and disclosure of information that could identify an individual. It attempts to mitigate these harms by providing transparency to individuals about how data is used, and requiring consent for many uses. However, this approach places an overwhelming burden on users navigating countless platforms. (ADM+S, sub. 14, p. 6).

But many consider that ‘privacy self-management’ does not achieve the goals of the Privacy Act. Based on a nationally representative survey of 1,000 Australians, the Consumer Policy Research Centre found that ‘only 7% of consumers agree that companies give consumers real choices to protect their privacy online’, with ‘52% of consumers finding it time-consuming to protect their privacy online’ (Gupta 2023b, p. 10).

Box 3.4 – What is the difference between flexible and outcomes-based regulation?

Flexible vs prescriptive

Flexibility refers to how much discretion entities have in the way they meet regulatory requirements. Requirements that do not allow flexibility are considered to be prescriptive. Flexible regulation is typically less onerous than prescriptive regulation as it provides regulated entities with choice about how they meet regulatory requirements. Although prescriptive regulation may increase certainty, it can also:

lock in inefficient practices and inhibit productivity by impeding flexibility and the take-up of new technologies, business models and processes ... [and] result in higher costs to government agencies (regulators) to administer and enforce. (Queensland Treasury 2022, p. 1)

Outcomes-based vs controls-based

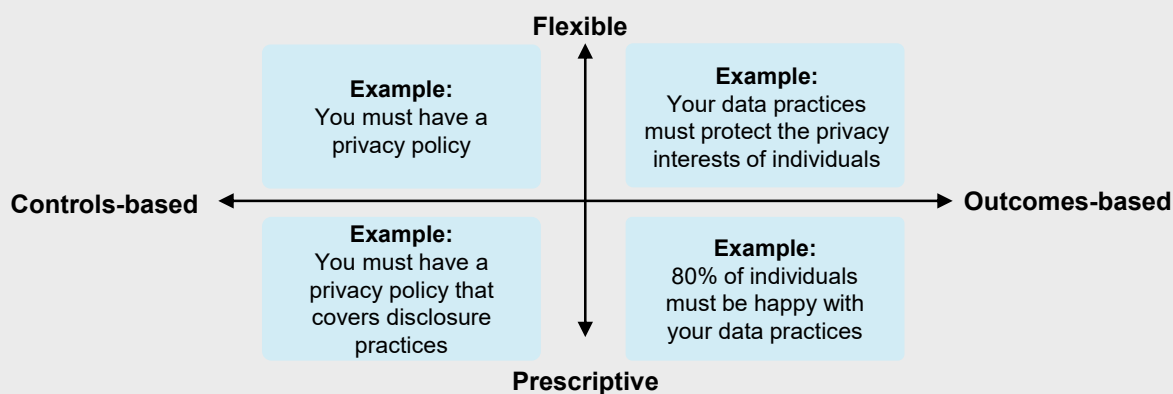
Some regulations are designed so as to require entities to achieve certain outcomes – these are known as outcomes- or risk-based regulations. Others prescribe or proscribe certain actions or procedures – these are controls- or inputs-based regulation. In general, outcomes-based regulation is preferable as it allows entities to choose the procedures or controls that are best suited to their business context.

Regulators, instead of focussing on prescribing the processes or actions that firms must take, should step back and define the outcomes that they require firms to achieve. Firms and their management will then be free to find the most efficient way of achieving the outcome required. (Black 2007, p. 5)

Outcomes-based regulation can also be more adaptable over time and ‘future-proof’ because it is agnostic about what processes and technologies are used to achieve the desired outcomes.

What does this mean for regulatory burden?

Regulation can be burdensome because it is too prescriptive, too controls-based, or both. As depicted in the diagram below, regulations that are flexible are not necessarily outcomes-based.



For example, in the context of the Privacy Act, the requirement in APP 1 to have a privacy policy is relatively flexible, as the privacy policy can contain whatever the regulated entity considers appropriate. But the underlying privacy outcome is about the alignment between how personal information is treated and what individuals expect or are informed of – and APP 1 prescribes the procedure through which this outcome is to be achieved.

Two methods of ‘privacy self-management’ were regarded as particularly ineffective – privacy policies, and consent and disclosure procedures. As IoT Alliance Australia submitted to this inquiry:

The balance is quite uneven for consumer and small business digital services where the blunt instrument of consent is often used as a ‘take it or leave it’ option. It is also unclear to consumers how any collected private data is shared (or not) with third parties, although this is often buried deep in often opaque and overlong privacy policies. (qr. 8, p. 1).

APP 1 requires regulated entities to have a clearly expressed and up-to-date **privacy policy** that outlines how it collects, uses, stores, and shares personal information. This is intended to enable individuals to make informed decisions about who they entrust with their personal information. In reality, privacy policies largely fail to effectively inform consumers of their rights.

- Most privacy policies are exceedingly lengthy and difficult to read – the typical privacy policy contains 6,876 words on average. ‘If Australian consumers were to read all of the privacy policies they encounter in full, it would take nearly 46 hours every month’ (ACCC 2024b, p. 6). Privacy policies are typically constructed this way so that they can be ‘future-proof’, allowing entities to maximise the scope of the data they can collect and its uses (Elvery and Tan 2025).
- Individuals are likely to either miss or misunderstand terms in privacy policies. These terms often permit the collection and use of personal information beyond what is reasonably necessary for the service or product provided (Kemp 2020).
- Many privacy policies also contain conflicting messages, such as stating in large letters that they would ‘never sell your data’ while adding that they reserve the right to sell that data as a ‘business asset’ in fine print, in a separately located policy (Harrison 2023).

The APPs also govern when and in what form **consent and disclosure** is required. These requirements are intended to enable individuals to make informed decisions. However, they can become a ‘tick box’ exercise – in which businesses comply with the letter of the law but not its intent (CHOICE 2020). In fact, overreliance on consent and disclosure mechanisms was said to produce perverse outcomes and result in ‘consent fatigue’¹¹ (CHOICE 2020, p. 4).

In this vein, in their submission to the Privacy Act Review, Microsoft argued that consent should not be the sole mechanism for enabling data access and use.

While [Microsoft] support the consideration of robust approaches to ensure that consent is valid and meaningful, there are other situations in which obtaining consent may be impractical or impossible. (2020, p. 6)

For this reason, some participants supported moving to a regime that would require regulated entities to act in a manner that protects the interests of individuals and consumers. As ADMS+S submitted to this inquiry:

Importantly, we think that reforms should be made to introduce a positively framed regulatory framework which shifts the onus away from customers and regulators, and towards the organisations who collect and handle the data; and who are almost always in the best position to mitigate related harms. (sub. 14, p. 8).

This approach could reduce the need for individuals to constantly ‘make informed and rational decisions with little market intervention’ to protect themselves from harm (Gupta 2023a, p. 4). A similar problem was faced in the financial services sector in relation to the management of conflict of interests by advisers and

¹¹ Consent fatigue refers to the ‘disengagement or mental exhaustion that consumers may experience when asked to comprehend technical or extensive information, or engage in multiple and repetitive interactions’ (Treasury 2023a, p. 7).

mortgage brokers, which led to the introduction of best interest obligations (box 3.5). This issue was also a key motivator for the recommendation in the recent Privacy Act Review to introduce a ‘fair and reasonable’ test that would apply to the collection, use and disclosure of information (discussed below) (AGD 2023d).

Box 3.5 – Financial services: replacing disclosure with a best interest duty

Prior to 2012, conflicts of interests in the financial services sector were managed via disclosure practices. These disclosure practices were intended to ensure that clients had adequate information to make an informed decision about financial products and services being sold to them. In practice, however, disclosures often failed to fully inform individuals.

In its Inquiry into Financial Products and Services in Australia, the Parliamentary Joint Committee on Corporations and Financial Services noted that:

disclosure documents are too long and confusing for conflicts of interest caused by commission-based remuneration and vertical ownership structures to be properly understood by consumers. The documents are so inaccessible that they are probably not read at all by most people. (2009, p. 87)

In 2012, a best interest obligation was introduced for financial advisers, requiring them to act in the best interests of their clients, beyond simply disclosing conflicts of interest. A best interest obligation for mortgage brokers was later introduced following the inquiry on Competition in the Australian Financial System (PC 2018) and the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry (Hayne 2019).

Renewing the focus on privacy outcomes

Regulation that focusses too heavily on controls, as opposed to outcomes, can dampen innovation. Even if the actions or procedures required by the regulation seem individually ‘sensible’, they may not be the only way to meet the regulatory objective and there is limited ability for regulated entities to find new ways to do things.

That said, moving away from controls-based requirements is *not* about redefining the privacy outcomes that are already articulated in the objects of the Privacy Act (s. 2A). In other words, it is not about prioritising innovation and productivity above privacy protections – rather, it is about achieving those privacy objectives in the most efficient and effective manner.

An alternative compliance pathway

One concern about the current Privacy Act regime is that it is not scalable – that is, it does not adapt according to risks posed by different uses of data and the size of different regulated entities.

Several submissions to the Privacy Act Review underlined the need for the Privacy Act to accommodate different business models (ARCA 2020, p. 6; Google 2020, p. 2; IGEA 2020, p. 6; The Guardian Australia 2020, p. 5). As the Australian Retail Credit Association argued, ‘the degree of emphasis on privacy protection must always consider context, because the appropriate degree of privacy protection cannot be set uniformly for all contexts’ (2020, p. 6). This is especially important in light of the proposed changes to expand the scope of the

Privacy Act to cover small businesses (Master Electricians Australia, qr. 51, p. 1). The Interactive Games and Entertainment Association emphasised the importance of ensuring that privacy regulation:

... accommodates different risk levels in terms of data and uses of data, rather than taking a 'one-size-fits-all' approach to regulation. For example, transparency and consent requirements should vary depending on the sensitivities and risks surrounding the type of personal data collected. (2020, p. 6)

Scalable regulation supports innovation by allowing regulated entities to pursue more efficient and cost-effective ways to meet regulatory objectives. As CHOICE said in the Privacy Act Review:

A performance-based model allows companies to innovate – they can experiment with how information is presented to achieve the best outcome. (2020, p. 4)

Similarly, as CPA Australia submitted to this inquiry:

Privacy law should not be viewed solely as a safeguard, but also as a foundation for innovation, inclusion, and public benefit in the digital economy. We encourage the Productivity Commission to consider privacy reforms that reduce unnecessary complexity, and focus regulation and regulatory efforts on high-risk areas. (qr. 45, p. 2)

To enable this, **the PC recommends the introduction of an alternative compliance pathway**. This would create a 'dual track' compliance regime, consisting of one outcomes-based track (designed to provide flexibility for regulated entities) and one more prescriptive track (designed to provide regulated entities with greater certainty about their privacy obligations). Regulated entities would be able to choose the mode of compliance that best suits their business needs. Importantly, this differs from the recommendation in the Privacy Act review to integrate a 'fair and reasonable' test within some of the existing APPs (table 3.1) – that proposal would impose *additional* requirements on the collection, use and disclosure of information (AGD 2023d, pp. 120–121), whereas this recommendation is about creating *alternative* requirements.

The creation of an alternative compliance pathway could also alleviate the incidence of over-compliance (that is, wasted compliance effort). For example, a business that is currently obtaining unnecessary consents might no longer do so, if it considered that it could satisfy privacy requirements through the alternative pathway instead. An alternative compliance pathway may improve privacy outcomes for individuals by '[shifting] the onus onto businesses instead of holding consumers accountable to search for their best interests in a market economy that hasn't been developed with their interests in mind' (Gupta 2023a, p. 8).

A dual-track compliance regime was supported by several participants in the Privacy Act Review. Specifically, some regulated entities supported the introduction of a safe harbour – a legal provision that protects entities from liability if they have failed to meet their legal obligations, provided they have taken certain prescribed actions.

the Act should remain principles based but [we] would support the APP Guidelines being amended to include specific 'safe harbour' provisions in certain areas. (AGL Energy 2020, p. 2)

Woolworths submits that greater certainty about the standard expected of businesses can best be achieved with the introduction of 'safe harbour' defences, which would apply, for example, where appropriate privacy impact assessments are undertaken and measures implemented to mitigate identified risks. (Woolworths Group 2022, p. 2)

In Australia, dual-track compliance regimes already exist in several other regulatory areas, including for financial advisors and work health and safety (box 3.6).

Box 3.6 – Examples of dual-track compliance regimes in Australia

Work Health and Safety (WHS) legislation and Codes of Practice

- **Outcomes-based compliance** – a person conducting a business or undertaking has a duty of care to ensure ‘so far as is reasonably practicable’, the health and safety of workers, including by managing risks based on outcomes, not prescribed steps (Safe Work Australia 2011, p. 3; Work Health and Safety Act 2011, s. 19). To achieve compliance using this pathway, entities must provide an ‘equivalent or higher standard of work health and safety than the code’ (Safe Work Australia 2011, p. 2).
- **Model Codes of Practice** – entities who follow Model Codes of Practice issued under the WHS Regulations will often be taken to be compliant with the work health and safety duties in a jurisdiction’s WHS Act and Regulations (Safe Work Australia 2011, 2025).

Product Safety and Electrical Equipment Standards

- **Outcomes-based compliance** – ‘AS/NZS 3820 prescribes outcomes-oriented safety criteria for electrical equipment’ (EESS 2025).
- **Technical standards** – compliance with the safety criteria in AS/NZS 3820 can generally be met by demonstrating compliance with the relevant standards (EESS 2025). Products can meet prescribed technical standards or demonstrate equivalent safety/performance through testing and certification.

Financial Advice Obligations (Best Interests Duty)

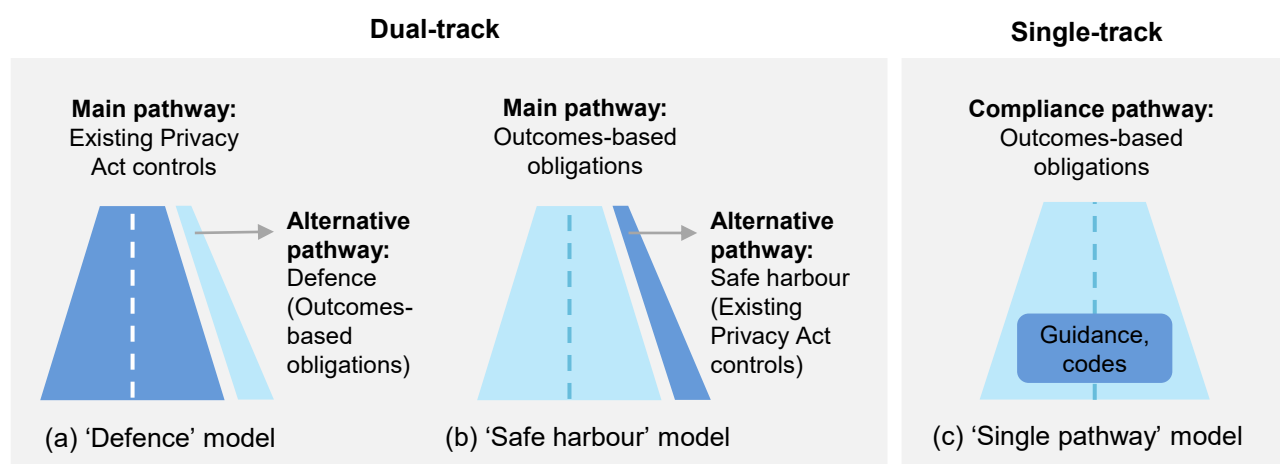
- **Outcomes-based compliance** – under s. 961B of the *Corporations Act 2001* (Cth), advisers must act in the best interests of the client.
- **Safe harbour^a** – the law provides a ‘safe harbour’ checklist (steps 1–7 under s. 961B(2)) which, if followed, deems the adviser to have met the duty.

a. The *Quality of Advice Review* found that, in practice, ‘financial advisers focus[ed] more on the safe harbour steps than the primary duty’ (Levy 2022, p. 86) and, for that reason, recommended that the safe harbour be removed.

Based on these existing regimes, the PC has identified two broad options for implementing a dual-track compliance regime in the Privacy Act.

- The outcomes-based obligations could be framed as a ‘defence’. This means that the existing Privacy Act requirements would be retained as the core regulatory regime, but regulated entities who do not (or choose not to), for example, meet all the current APPs to the letter, could invoke the defence to show that they are nevertheless compliant with their regulatory obligations (figure 3.1, panel a).
- The outcomes-based requirements could be framed as the general rule that applies to all regulated entities. The existing Privacy Act requirements (including the APPs) could be cast as a safe harbour or ‘deemed to satisfy’ style regime – so regulated entities could opt to follow a more prescriptive or controls-based set of rules that would be deemed to meet the broader outcomes-based obligation (figure 3.1, panel b).

In essence, these options are inversions of each other – reversing which path is the ‘rule’ and which path is the ‘exception’. This means that choosing between these options is an implementation issue, not one of policy. The PC favours the defence model, because it would be an extension of the existing privacy framework, rather than a foundational change. Creating a new defence would require relatively discrete amendments to the Privacy Act, compared to implementing a safe harbour model. This is compounded by the fact that the APPs are a mix of principles and controls-based requirements, meaning that they could not be used in their current form to create a safe-harbour pathway.

Figure 3.1 – Design options

The PC also considered the option of reorienting the Privacy Act regime, as a whole, towards an outcomes-based approach. This would entail retaining a single-track compliance pathway in which outcomes-based requirements would replace all existing controls-based privacy requirements. This could be supplemented by codes or regulatory guidance material to provide additional clarity and certainty for regulated entities (figure 3.1, panel c). However, like the safe harbour model, this approach was not preferred, as it would require more comprehensive changes to the Privacy Act's legislative architecture.

Options for framing requirements for the alternative pathway

The overarching objective of privacy regulation is to protect the privacy interests of individuals and/or to prevent or reduce harm resulting from privacy breaches. Therefore, an alternative compliance pathway should require regulated entities to meet broad obligations in relation to this objective.

There are several options for how outcomes-based obligations could be framed, modelled on obligations that already exist in other regulatory areas or have been recommended for adoption for data and digital technologies (box 3.7). These could be adapted to create a similar duty or obligation in relation to privacy.

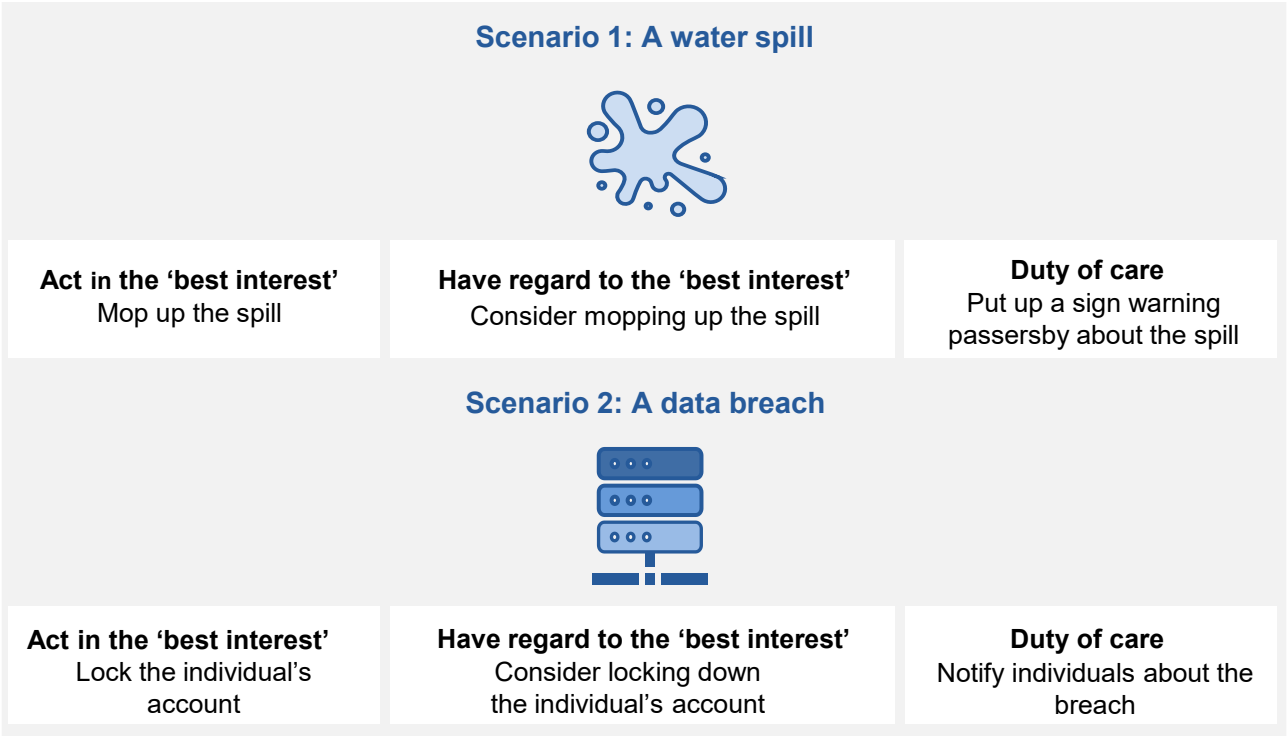
- A **best interest obligation** would require regulated entities to act in the best interest of an individual in respect of their privacy. In other words, the regulated entity, when making decisions about how to act, would be required to prioritise the privacy interests of individuals.
- An obligation for regulated entities to **have regard to the best interest** of an individual in respect of their privacy. That is, the regulated entity, when making decisions about how to act, would be required to consider the privacy interests of individuals, but not necessarily prioritise those interests.
- A **duty of care** would require regulated entities to take steps to prevent reasonably foreseeable harm to an individual's privacy. This would involve taking steps to identify potential harms and prevent or mitigate those harms.

Figure 3.2 illustrates how these obligations and duties impose different requirements in the context of a water spill and a privacy breach.

Box 3.7 – Examples of duties and obligations

- In financial services, **best interest obligations** apply to some types of service providers, and require them to prioritise and act in the best interests of their client. For example, Pt 3-5A of the *National Consumer Credit Protection Act 2009* requires mortgage brokers to act in the best interest of their client (ASIC 2020, p. 1). This obligation is framed as high-level principles and outcomes such as that ‘the obligations should lead to a higher quality of credit assistance being provided’ (ASIC 2020, p. 6).
- **The forthcoming digital duty of care** will require digital platforms ‘to take reasonable steps to prevent foreseeable harms on their platforms and services’ (Rowland 2024).
- **A best-interest duty specific to children’s privacy** was proposed in the 2023 Privacy Act Review. This best-interest duty would ‘require entities to have regard to the best interests of the child as part of considering whether a collection, use or disclosure is fair and reasonable in the circumstances’ (AGD 2023d, p. 10).

Figure 3.2 – The requirements of the different obligations^a



a. These scenarios are illustrative of what sorts of actions may be sufficient to meet the relevant duty or obligation.

The PC’s preliminary view is that a best interest obligation would be the best path forward. We are seeking feedback on which model should be preferred over others – and, if so, why.

How should enforcement occur?

At present, enforcement of the Privacy Act is largely the responsibility of the regulator, the Office of the Australian Information Commissioner (OAIC). An alternative or complementary option would be to enable individuals to enforce their rights directly.

A related issue is the capacity and capabilities of these parties to undertake enforcement actions – and whether additional resourcing or regulatory architecture is needed to enable effective regulatory activity. This is particularly acute given the shared expectation that the OAIC provide clear guidance to support both individuals and entities.

clear guidance must be issued by the OAIC well in advance of any changes being enacted and be developed with input from industry on the drafting to ensure they are addressing any operational ambiguities. (Insurance Council of Australia, qr. 29, p. 2)

In this vein, the Privacy Act Review considered funding arrangements for the OAIC, as well as the case for extending existing external dispute resolution schemes, the creation of a privacy ombudsman and the establishment of a Deputy Commissioner for Enforcement (AGD 2023d, pp. 265–271). There could also be mechanisms for enforcement in other regulatory areas that could be adopted in the context of privacy – such as the super complaints (designated complaints) mechanism under the Australian Consumer Law (ACCC 2024a).

The PC is seeking feedback on how enforcement of an outcomes-based obligation should occur and if any other changes would be needed to enable effective enforcement.



Draft recommendation 3.1 An alternative compliance pathway for privacy

The Australian Government should amend the *Privacy Act 1988* (Cth) to provide an alternative compliance pathway that enables regulated entities to fulfil their privacy obligations by meeting criteria that are targeted at outcomes, rather than controls-based rules.



Information request 3.1

The PC is seeking feedback on implementation issues, including how an alternative compliance pathway should be embedded in the *Privacy Act 1988* (Cth).

- What are the anticipated costs and benefits of implementing an alternative compliance pathway?
- How should an alternative compliance pathway be designed – through the creation of a new defence, a safe harbour, deemed-to-comply standards, or something else? Why?
- How should requirements for the alternative pathway be framed – as a duty of care, a fiduciary duty, a best interest obligation, or something else? What are the merits and downsides of the different options?
- How should those obligations be enforced? Are any other changes needed to enable effective enforcement?

Proposed reforms risk entrenching existing problems

The recent Privacy Act Review made 116 recommendations to reform the Privacy Act, following three general themes (key recommendations are set out in table 3.1).

Table 3.1 – Key recommendations from the Privacy Act Review

Scope and application of the Act	Protections	Regulation and enforcement
Amend the objects of the Act to clarify that the Act is about the protection of personal information	Require the collection, use and disclosure of personal information be fair and reasonable in the circumstances	Strengthening the enforcement powers of the Information Commissioner
Broaden the definition of personal information to encompass technical and inferred information	A right to erasure of personal information	New civil penalties , including a ‘mid-tier civil penalty’ for breaches that are not serious or repeated
Amend the definition of sensitive information to include genomic information	A right to object to an entity processing their personal information in certain circumstances	A direct right of action for individuals to take court action for interference with privacy
Remove the small business exemption	New protections for children including a Children’s Online Privacy Code	A statutory tort for serious invasions of privacy

Source: Attorney-General’s Department (2023d).

Some reforms have already been implemented

Some of the recommended reforms were passed in the *Privacy and Other Legislation Amendment Act 2024* (Cth) including:

- introducing a statutory tort for serious invasions of privacy
- introducing a mandate for the OAIC to develop a Children’s Online Privacy Code
- granting the OAIC new powers to issue infringement and compliance notices, which may give rise to the imposition of civil penalties (Parliament of Australia 2024).

It is anticipated that further reforms will be implemented through a second tranche of legislative changes. These reforms are anticipated to include requiring entities to undertake privacy impact assessments for high-risk activities (including automated decisions), introducing the ‘fair and reasonable’ test, abolition of the small business exemption and changing the definition of ‘personal information’ (Helios Salinger 2022; McGrath et al. 2024).

Some anticipated reforms could exacerbate the regulatory burden

During consultation for the Privacy Act Review, concerns were expressed that some anticipated reforms could increase the complexity of the Act and add to the regulatory burden. For example:

My overarching concern with the Issues Paper, and the proposals from the Digital Platforms Inquiry that preceded it, is that they reflect an orientation towards tweaking specific rules - and adding more. This will contribute to a privacy regime in Australia that is already too complex and fragmented. (Weatherall 2020, p. 1)

The proposals – including some that were enacted in the first tranche – were said to exacerbate the cumulative regulatory burden of the Act.

If all or most of the potential reforms ... were implemented, the overall effect would be to increase the regulatory obligations on the ABC and other entities subject to the Privacy Act. The ABC would require time, funding and additional appropriately skilled personnel in order to resource the redesign of the ABC's systems and processes to comply with the new laws. (ABC 2020, p. 3)

Similarly, the Information Technology Industry Council highlighted how these proposals could increase business costs and affect competition.

We believe that some proposals for the review of the Act could unintentionally constrain the ability of Australian and other companies to operate fully in the market, while in some cases offering limited incremental benefit to Australian citizens' privacy. (2020, p. 1)

In addition, participants expressed concern about the cost-benefit analysis that was undertaken for the Privacy Act Review. One concern was about lack of transparency about whether the anticipated benefits of reform would outweigh the costs – the cost-benefit analysis has not been released publicly, despite requests that it be tabled in Parliament (McLachlan 2024, p. 2). There were also concerns about the methodology used (box 3.8), and that it would lead to unreliable estimates of the likely costs and benefits. Participants in this inquiry also said that the lack of transparency about which reforms would be implemented further contributed to an environment of uncertainty for businesses (Woolworths, sub. 7, p. 2).

Another area of concern were the recommended reforms that would bring Australia's privacy regime in line with the General Data Protection Regulation (GDPR), which has stifled firm productivity and innovation in the European Union (box 3.9).

We caution against the wholesale importation of GDPR. The GDPR, notably its enforcement penalties are widely regarded as draconian. Australia should avoid the excessive costs of the GDPR regulations (AFMA 2020, p. 1)

Box 3.8 – Concerns about the cost-benefit analysis for the Privacy Act Review

Multiple parties who had been consulted on the draft cost-benefit analysis told the PC that they were concerned about the methodology that was used. In a joint letter to the Attorney-General's Department (released under a Freedom of Information request), 12 industry associations (including the Australian Banking Association, the Business Council of Australia, and the Tech Council of Australia) said:

We have fundamental concerns with the approach and methodology ... including the formulation of the assumptions, the mischaracterisation of some of the perceived benefits and the failure of the [cost-benefit analysis] to adequately capture the likely costs to industry associated with the operationalisation of the reforms. (2024, p. 1)

The associations urged that 'Government considers revising its approach as the current methodology and scope of the [cost-benefit analysis] will not provide Government with an adequate understanding of the costs of implementing potential reforms' (ABA et al. 2024, p. 1). They submitted that the failure of Government to respond to these limitations may have contributed to poorly designed recommendations that place unnecessary costs on entities (ABA et al. 2024).

Box 3.9 – How has the GDPR affected European businesses

The General Data Protection Regulation (GDPR) sets the most comprehensive standards for privacy protection in the world, backed by large fines for non-compliance (Wolford 2019). Requirements include certain firms having to have a data protection officer, a right to erasure and stricter consent processes.

Compliance with the GDPR has proven costly for firms, as well as difficult. One survey of privacy-active firms by IAPP and EY (2018, p. 80) found an average transition cost above US\$3 million for firms with at least 5,000 employees. These costs had anticompetitive effects, with smaller firms facing a proportionally higher burden (Ponemon Institute 2018, p. 22).

At the aggregate level, evidence indicates that the adoption of the GDPR has dampened economic activity. Relative to the United States, firms in Europe reduced data storage by 26% (Demirer et al. 2024), technology venture investments declined by 24% (Jia et al. 2021, p. 4) and the profits of data-intensive European firms declined by 1.9 percentage points (Koski and Valmari 2020, table 3a). Compared to the situation prior to the adoption of GDPR, e-commerce also declined (Goldberg et al. 2024, pp. 354–355). The available evidence suggests the GDPR has imposed considerable economic costs on firms and consumers in Europe and beyond.^a

Especially concerning is the reduction in innovation caused by the GDPR. For instance, Janssen et al. (2022) found that the adoption of the GDPR reduced the entry of apps into the global market by half. There is evidence that, in response to the introduction of the GDPR, the innovation mix shifted away from the radical, new-to-market innovations that contribute to large productivity gains, and toward less impactful, incremental innovation (Blind et al. 2023, pp. 24–25).

a. The economic evidence has some limitations that affect the magnitude of the estimates in both directions. First, most evidence is short-term, and effects may have reduced over time as firms have adapted. Second, some of the effects detected may have been due to changing market concentration, although this cannot explain the overall results. Third, many US firms were also impacted by GDPR, meaning some effects may be underestimated.

One example of this is the proposal to introduce a right to erasure, modelled on the corresponding GDPR right (AGD 2023d). In essence, this would be ‘a right to have information deleted’ (AGD 2023d, p. 166), with the following features:

- (a) An individual may seek to exercise the right to erasure for any of their personal information.
- (b) An APP entity who has collected the information from a third party or disclosed the information to a third party must inform the individual about the third party and notify the third party of the erasure request unless it is impossible or involves disproportionate effort.
- (c) In addition to the general exceptions, certain limited information should be quarantined rather than erased on request, to ensure that the information remains available for the purposes of law enforcement. (AGD 2023d, p. 176)

Many regulated entities shared concerns about the regulatory burden and implementation barriers associated with the right to erasure. Submitters to the Privacy Act Review suggested that this reform is rooted in an abstract – and ostensibly ‘appealing’ – idea about rights, and has little regard for the practicalities of implementation, or its actual costs and benefits (Communications Alliance Ltd 2020, p. 10).

The Australian Broadcasting Corporation suggested that ‘this reform could place a significant regulatory burden on media organisations’ (2020, p. 6). Optus also said:

There are significant technical hurdles to implement this for most sectors of the economy and much more research needs to be conducted. Implementation should only be considered if there is a quantifiable overall benefit. (2020, p. 11)

AGL said it was unclear whether the benefits to individuals would outweigh the costs.

Without further cost-benefit analysis it is not clear what the additional benefits for consumers would be if the full right to erasure was introduced, and whether these benefits would outweigh the risks and the potentially significant costs to business. (2020, p. 4)

Some participants in the Privacy Act Review also queried the need for a right to erasure, given that there are already requirements that result in substantively similar outcomes for individuals.

We do not believe a right to erasure is required, given APP 11 already requires that where an APP entity no longer needs personal information for any purpose for which the information may be used or disclosed under the APPs, the entity must take reasonable steps to destroy the information or ensure that it is de-identified. (Telstra 2020, p. 17)

These concerns reflect the experience of firms in the European Union, which consistently rated the right to erasure (also known as the right to be forgotten), as the hardest obligation to implement under the GDPR (IAPP and EY 2018, p. 64, 2019, p. 58).

In light of these concerns, any further reforms to implement the recommendations of the Privacy Act Review should be undertaken with a degree of caution. In particular, the merits of any contemplated reforms should be evaluated with a critical eye trained on the practical impacts of reform – that is, the benefits to individuals, as well as the costs to regulated entities and the resultant effect on innovation and productivity. On this basis, the PC considers that a GDPR style right to erasure as described in the Privacy Act Review and the Government response to the Privacy Act Review should not be implemented in Australia.



Draft recommendation 3.2 **Do not implement a right to erasure**

The Australian Government should not amend the *Privacy Act 1988* (Cth) to introduce a ‘right to erasure’, as this would impose a high compliance burden on regulated entities, with uncertain privacy benefits for individuals.

4. Enhance reporting efficiency, transparency and accuracy through digital financial reporting

Summary

- * **Digital financial reporting has the potential to increase the efficiency, transparency and accuracy with which the data in financial reports is prepared, extracted and analysed.**
 - Report preparers and users – including companies, investors, auditors and government agencies – could complete existing activities more accurately and with fewer resources, as well as undertaking new activities.
- * **These benefits have not materialised in Australia, as no digital financial reports have been submitted. This is despite it being possible to voluntarily lodge digital financial reports since 2010.**
- * **Australia is an outlier, with many other jurisdictions – including the United Kingdom, United States, European Union, Japan and South Korea – having mandatory digital financial reporting schemes.**
- * **Digital financial reporting should be the default in Australia.**
 - International evidence indicates that digital financial reporting is only adopted widely when it is mandated.
 - This is likely due to the upfront costs of transitioning to digital financial reporting for report preparers, the limited benefits associated with only a small number of digital financial reports being submitted and the fact that it is currently mandatory to submit non-digital hard copy or PDF financial reports.
 - Artificial intelligence and other digital technologies are a complement to, not a substitute for, digital financial reporting – these tools need the structure of a digital financial reporting taxonomy to work effectively.
- * **A transition to digital financial reporting would require report preparers and users to update their systems and processes.**
 - While there would be costs associated with this, particularly for report preparers, the available evidence suggests that these costs are not excessive, are falling over time and are lower than the costs of non-digital report preparation in the long run.
 - And report preparers stand to benefit from improved business information processing, such as for performance benchmarking purposes, provided that enough digital financial reports are submitted.
- * **The Productivity Commission is seeking feedback on how mandatory digital financial reporting could best be implemented for disclosing entities as defined in the Corporations Act, which encompasses publicly listed companies and other public interest entities.**

We are forgoing the benefits of digital financial reporting

Most Australians undertake some form of financial investment, whether directly through share ownership, or indirectly via superannuation. The Australian Government also makes financial investments on behalf of Australians through instruments such as the Future Fund. Financial reports inform these investment decisions by providing critical insights into a company's financial performance.

Australia is one of only a few countries where financial reports continue to be submitted in a non-digital format, such as hard copies or PDF files, as standard practice. Consequently, extracting and analysing data from Australian financial reports is expensive, time-consuming and can be prone to error.

Digital financial reporting, where reports are prepared in a format that is more efficient for data extraction and analysis, is mandated in almost all the world's other major capital markets. Introducing a similar mandate in Australia would be accompanied by transition costs for report preparers and users. However, in the long term, this shift has the potential to raise productivity by increasing the efficiency, transparency, accuracy and accessibility of financial reporting.

Financial reports are a key source of financial information

In Australia, the *Corporations Act 2001* (Cth) is the main legislation governing corporations and financial markets, products and services. The Act mostly applies to companies operating in Australia, but can also apply to other types of entities, including partnerships and managed investment schemes (AICD 2025). The Act – and the accompanying Corporations Regulations 2001 (Cth) – sets out the way a corporation must be established, run and wound up to be compliant with the law. For some entities, such as **reporting entities** and **disclosing entities**, this includes a requirement to prepare financial reports (box 4.1). Compliance with the Act is overseen by the Australian Securities and Investments Commission (ASIC) (s. 5B).

Financial reports are one component of an annual report – the key means through which an entity informs interested parties, such as shareholders and analysts, about their activities, finances and strategies (box 4.1). Financial reports can be prepared in a non-digital format (for example, hard copy, PDF file or HTML file) or a digital format. It is mandatory in Australia to submit financial reports in a non-digital format (hard copy or PDF file), while digital reports can be submitted voluntarily (ASIC 2025a).

Non-digital financial reports are designed to be read by people, but it is difficult for either people or computer applications to extract and analyse large volumes of information from them. In contrast, **digital** financial reports are prepared in a format that is more efficient for data extraction and analysis, while also having the capacity to retain the readability of a non-digital report. Digital financial reports use 'tags' to assign meaning to financial information, where each tag is defined within a broader taxonomy of tags that is based on accounting standards (box 4.2).

As well as traditional financial reports, requirements for some Australian entities to lodge sustainability reports are being phased in from 1 January 2025. The Australian Sustainability Reporting Standards require entities to 'disclose information about climate-related risks and opportunities that could reasonably be expected to affect the entity's cash flows, its access to finance or cost of capital over the short, medium or long term' (AASB 2024a, para. 2). Entities can choose to voluntarily disclose all broader sustainability-related risks and opportunities that may affect their finances (AASB 2024b, para. 3). ASIC is finalising arrangements for the lodgement of sustainability reports – the reports will be submitted in a non-digital format (ASIC, personal communication, 18 July 2025).

Box 4.1 – What are financial reports and annual reports, and who prepares them?

Under section 292 of the Corporations Act, some entities are required to prepare financial reports. Financial reports are one part of an annual report and provide information about an entity's financial performance and position. There are different reporting requirements for different entities.

Financial reports must be prepared in accordance with Australian Accounting Standards (s. 296(1)) and there are legal consequences if the information contained within them is materially false or misleading (s. 1308). The reports are used by the Australian Securities and Investments Commission (ASIC) to monitor compliance with standards and regulations and to detect potential financial mismanagement.

Reporting entities An entity for which 'it is reasonable to expect the existence of users dependent on general purpose financial reports for information' (Statement of Accounting Concept 1, para. 40).

Includes disclosing entities (incorporated or formed in Australia), public companies (except small companies limited by guarantee), large proprietary companies, registered schemes and some small proprietary companies (s. 292).^{a,b,c}

Disclosing entities A subset of reporting entities (s. 111AC). They are subject to a certain level of public interest and therefore have enhanced disclosure requirements, including a requirement to submit half-yearly reports (s. 111AO) and continuous disclosure requirements (s. 111AP).

Includes entities and registered schemes that are listed, raise funds pursuant to a disclosure document or Product Disclosure Statement, offer securities other than debentures as part of a takeover scheme or offer securities under a compromise or scheme of arrangement (ss. 111AE–111AI).

Listed companies One type of disclosing entity. These companies may have additional reporting requirements. For example, ASX-listed companies must make disclosures as per ASX Listing Rules and include a Corporate Governance Statement in their annual report.

Includes companies listed on stock exchanges such as the ASX, NSX and SSX.

a. These lists are not exhaustive. **b.** A company is 'large' if it meets at least two of three thresholds: consolidated revenue of \$50 million or more, consolidated gross assets of \$25 million or more and 100 or more employees (Treasury 2019). **c.** Small proprietary companies must prepare financial reports if they are foreign-controlled, or if they had one or more crowd-sourced funding shareholders at any time during the financial year.

COMPONENTS OF AN ANNUAL REPORT

Directors' report (ss. 298–300) A comprehensive overview of the entity's activities, finances and strategies during the reporting period. The directors' report provides narrative context for other sections of the annual report, including the financial report.

Financial report (s. 295) Information about financial performance and position, including four key financial statements (covering the current and preceding period), notes to the financial statements and a directors' declaration.

Auditor's report (s. 308) The auditor's opinion on whether the financial report gives a true and fair view of the entity's reported financial position and performance and complies with regulations and standards.

Corporate Governance Statement (for ASX-listed companies) Discloses the extent to which the entity has followed the ASX Corporate Governance Council's non-mandatory principles and recommendations (or explains why they have not done so).

Box 4.2 – Why it is easier to extract and analyse data from digital financial reports

Extracting and analysing data from financial reports is more efficient with digital reporting relative to non-digital reporting. This is because digital reporting uses 'tags' to assign meaning to the financial information in reports, where each tag is defined within a broader taxonomy of tags that is based on accounting standards.^a

For example, a non-digital version of a financial report may identify a company's Current Assets in 2023-24 as \$1,160,000. In a digital financial report, the company's \$1,160,000 of Current Assets would be tagged as `<CurrentAssets contextRef='e2024' unitRef='Australian dollar'>1160000 </CurrentAssets>`. Essentially, the 1,160,000 would be recognised by computer applications as Current Assets of 1,160,000 in Australian dollars for 2023-24. This value could then be compared with the same tag in other companies' financial reports.

a. For example, 'a taxonomy can define that Total Assets are comprised of Current and Non-current Assets ... Similarly, taxonomies can define calculation-based relationships, such that, for example, Gross Profit is calculated as the difference between Revenue and Cost of Goods Sold'.

Source: Troshani and Rowbottom (2022, p. 5).

Digital financial reporting would benefit report preparers and users

In Australia, the option to voluntarily submit digital financial reports has been available since 2010, but as of June 2025, no digital financial reports have been submitted (ASIC, sub. 2, p. 1). This means that both report preparers and report users – like companies, regulators, investors, analysts and auditors – are missing out on the benefits of digital financial reporting (figure 4.1).

In 2023, Deloitte Access Economics reported that the long-term annual net benefit of mandating digital financial reporting was estimated to be \$7.7 billion (2023, p. 13). This was estimated on the basis that the mandate would apply to all businesses with over \$50 million in annual revenue (one of the three thresholds that defines a 'large company', with large companies needing to meet two of these three thresholds) (box 4.1; Deloitte Access Economics 2023, p. 28).¹²

¹² The modelling estimates the impact of a digital financial reporting mandate using, in some instances, costs and benefits associated with similar reforms overseas that, despite being the best available evidence, may not be fully applicable to the present-day Australian context.

Figure 4.1 – The benefits of digital financial reporting would accrue to multiple parties

	Improvements to existing activities	Enabling of new activities
Report preparers	Better business information processing (for example, as part of performance benchmarking)	Visibility of report preparers in global capital markets
Report users ^a	Less time-consuming and more accurate data extraction and analysis	'Big data' analysis
Auditors	Earlier detection of anomalies and emerging financial issues	Novel data-driven audit methodologies
Regulators and other government agencies	More effective risk targeting (such as in audit inspections)	New enforcement approaches Estimating impacts of changes to accounting standards

a. Such as shareholders, investment firms, data aggregators, financial analysts and researchers. Report preparers, auditors, regulators and other government agencies are also report users but are considered separately here.

Existing activities require fewer resources and are done more accurately ...

Information in financial reports can be processed more efficiently and accurately when it is in a digital, machine-readable form (box 4.2). This gives rise to two sources of productivity growth (PC 2023c, p. 5). First, the extraction and analysis of information from financial reports becomes *cheaper*, as the number of hours of workers' time needed to complete a particular task – such as extracting data from a statement of cash flows – falls. Second, the improved quality of extraction and analysis means that these activities are completed in a *better* way.

For **auditors**, for example, it is easier to extract and transform data from digital financial reports, leaving more time for analysis (Perdana et al. 2015, p. 125). More broadly, increased access to digital financial information will allow auditors to 'identify anomalies, detect potential fraud, and uncover emerging financial issues at an earlier stage' (CA ANZ 2025, p. 9).

Transitioning to digital financial reporting would reduce information processing costs for **report users** such as investors, investment firms, data aggregators, financial analysts and researchers.

As one example, data aggregators often maintain their own internal data taxonomies so reports that have been prepared under different jurisdictions' reporting standards can be better compared. When financial reports are prepared in a non-digital format, data aggregators judge how each line item in a non-digital report maps to their own taxonomy. In contrast, when financial reports are prepared digitally, the information within them has already been assigned meaning from the 'tags' of a digital reporting taxonomy (box 4.2). Consequently, aggregators working with digital reports can systematically map data from the taxonomy used to prepare the report to their internal one (as opposed to manually mapping line items) (ASIC 2021). This

means that data can be extracted from financial reports more quickly and accurately. Report preparers then also receive the benefit of their financial information being represented more accurately in data aggregators' products (ASIC 2021).

More generally, an improved capacity to extract and analyse information from financial reports would be expected to lead to more informed decision making in capital markets. Globally, Tawiah and Borgi (2022) found that across 98 countries, the adoption of digital financial reporting was associated with improved financial reporting quality (as measured by the World Economic Forum's strength of auditing and reporting standards index).

However, evidence regarding the impact of mandatory digital financial reporting on report users' information processing capacity is mixed. Blankespoor et al. (2014, p. 1468) found that the introduction of mandatory digital financial reporting for listed companies in the United States did not initially reduce the information processing costs of small investors relative to large investors, whereas Bhattacharya et al. (2018, p. 60) identified an improvement in small investors' responsiveness to the release of financial information. Ultimately, in their review of existing research, Troshani and Rowbottom (2021, p. 220) concluded that 'there is consistent evidence that capital market indicators have changed after [digital financial reporting] was mandated'. The authors asserted that this represented improved communication of financial information between listed firms and capital market participants as a result of mandatory digital financial reporting.

For **report preparers**, digital financial reporting would facilitate improved business information processing (CA ANZ and Wells 2020, p. 4).

This evidence on the diversity of benefits associated with digital financial reporting for different parties is consistent with views shared by inquiry participants (box 4.3).

Box 4.3 – Participants identified a range of benefits of digital financial reporting

I regularly use information in financial reports as part of my employment and private research. My most common direct uses include obtaining details of a particular situation or industry practice ... If [financial] information was in a digital financial reporting format ... this would save time and effort, and increase the quality of research. (David Hardidge, qr. 19, pp. 2–3)

We use the information in financial reports to identify if corporations are paying the taxes they are required to pay and to identify subsidiaries in secrecy jurisdictions ... Digital reports would assist in conducting such analysis. (Tax Justice Network Australia, qr. 42, p. 2)

The Australian Digital Health Agency uses information in financial reports to assess potential vendor financial health during procurement activities and for benchmarking activities. [Having financial reports in a] digital format would allow for easier comparison and analysis. (Australian Digital Health Agency, qr. 16, p. 7)

Digital financial reporting would improve data consistency, accessibility and comparability to benefit a broad range of users in their decision making ... automated data extraction [would enable] more efficient, consistent and targeted analysis. (EY Australia, qr. 27, p. 2)

The value in digital financial reporting is in the ability of investors and other decision makers to compare consistently across companies. (CA ANZ, qr. 30, p. 3)

Government agencies are also confident they would benefit from greater uptake of digital financial reporting. ASIC identified that the capacity to extract data from digital financial reports would ‘provide more current, consistent and accurate information for risk-based targeting in ASIC surveillances’ (sub. 2, p. 2) (for example, as part of audit inspections). Digital financial reporting would also enable the Australian Accounting Standards Board (AASB) to more effectively evaluate the potential impact of changes to accounting standards. AASB’s submission to the Parliamentary Joint Committee on Corporations and Financial Services inquiry into the Regulation of Auditing in Australia stated that:

at present, it is very difficult to obtain accurate information on how many entities in Australia might be applying particular accounting policies and their significance, or the type of financial statements prepared. (2019, p. 13)

Evidence from taxation reporting suggests that there are sizeable benefits associated with a shift to digital reporting. The Australian Government’s 2010 Standard Business Reporting (SBR) reforms made it possible for report preparers to submit many taxation, financial and prudential reports in a digital format (PC 2012, pp. 103, 111). By 2012, the Australian Taxation Office (ATO) had publicly committed to making digital reporting the ATO’s ‘primary channel’ of communication over the coming years, with some non-digital reporting channels being phased out (PC 2012, p. 117). The ATO estimated that the 15 million digital reporting transactions made via their SBR-enabled practitioner lodgement service in 2014-15 saved report preparers and government \$400 million, with benefits rising to \$1.1 billion in 2015-16 (Cowan 2016). The use of SBR for taxation purposes has continued to accelerate: 593 million and 1.3 billion SBR transactions had been made by 2019 and 2022, respectively (ATO 2023, p. 7).

Mandatory digital reporting of payroll information using Single Touch Payroll-enabled software has also been gradually implemented since July 2018 (ATO 2021). The introduction of Single Touch Payroll was expected to deliver \$2.1 billion of savings to the Australian Government over the five years from 2018-19 (Australian Government 2019, p. 158).

... and digital financial reporting potentially enables further innovations

Most businesses in Australia do not innovate in the form of new to the world innovation. Rather, they adopt and adapt existing technologies. This is an important driver of productivity in the Australian economy (PC 2023a, p. x). Digital financial reporting is one example of this type of innovation, as Australia’s adoption of the technology lags almost all other major capital markets.

Digital financial reporting is mandated in jurisdictions that together cover more than 90% of global market capitalisation, including the United Kingdom, United States, European Union, Japan and South Korea (Deloitte Access Economics 2023, p. 6; IFRS Advisory Council 2022, p. 16).¹³ As a result, the cost of extracting data from financial reports is higher in Australia than elsewhere, and this has consequences for **report preparers**. XBRL International (2024) summarised the issue as:

Australia needs to catch up with much of the rest of the world ... Australian corporates currently have exactly zero digital visibility.

Similarly, CA ANZ (2025, p. 3) argued that without a transition to digital financial reporting:

Australia’s capital market is rendered effectively invisible or at best inaccurately viewed through continued use of paper and online PDF financial reporting.

¹³ The only comparable jurisdiction that also takes a voluntary approach is Canada (CA ANZ 2025, p. 6).

Because extracting data from non-digital reports is time-consuming, when Australian financial reports are released, data aggregators may be forced to prioritise collecting and presenting information from Australia's largest publicly listed companies. The information from smaller publicly listed companies is then provided in a less timely, complete or accurate fashion (or in a worst-case scenario, not provided at all) (XBRL International, personal communication, 2 July 2025).

A shift to digital financial reporting will give **report users** access to large volumes of data (Deloitte Access Economics 2023, p. 12). Evidence from the United States suggests that report users have taken up the opportunity to conduct 'big data' research and analysis enabled by digital reporting. Between 2010 and 2015, almost 90% of the 2.3 billion search requests to Electronic Data Gathering, Analysis and Retrieval (EDGAR) – the database system where publicly listed entities file digital reports – were made by IP addresses identified as 'robots', with these robots often being part of projects that involve compiling and analysing large datasets (Hollander and Litjens 2022, pp. 8–9, 52).

For **auditors**, digital reporting will encourage innovations such as 'data-driven audit methodologies' that are anticipated to make audit outcomes more precise and reliable (CA ANZ 2025, p. 8).

Digital financial reporting also offers new opportunities for **regulators**. Digital financial reporting has allowed the US Securities and Exchange Commission (US SEC) to analyse their entire collection of submitted reports, including conducting automatic checks for missing disclosures and making aggregate queries relating to specific disclosures (such as gathering all reported research and development expenditures) (ASIC 2021).

There is unmet demand for digital financial reports

Australian financial report users are keen to have greater access to digital financial reports. In Chartered Accountants Australia and New Zealand's (CA ANZ's) most recent survey of retail investors, about 70% of investors supported making digital financial reporting mandatory, with more than half saying greater availability of more customised, digital financial information would improve their ability to access financial information 'greatly' or by 'quite a bit' (2024, p. 12). The Australian Shareholders' Association was also supportive of wider adoption of digital financial reporting for listed companies, stating that it would deliver five primary benefits to shareholders: efficiency and accuracy, improved data quality, transparency and accountability, regulatory alignment and cost and analytical benefits (such as less costly data processing) (sub. 44, pp. 1–2). Other report users, including multiple Australian Government agencies, accounting bodies, auditors, and researchers have also stated their demand for digital financial reports.¹⁴

Digital financial reporting should be the default

To capture the benefits of digital financial reporting, the Productivity Commission recommends that it should be mandated. The mandate should initially cover disclosing entities as defined in the Corporations Act, which includes publicly listed companies and certain other public interest entities (box 4.1).

The benefits of digital financial reporting are likely to be largest for this group of report preparers, as the pool of report users not only includes regulators and auditors, but analysts and investors too. Similarly, the costs of transitioning to digital financial reporting will be relatively lower for disclosing entities (CA ANZ 2025, pp. 18, 21); some are dual-listed companies that prepare digital financial reports in other jurisdictions, while others are already using software that can prepare digital financial reports (Workiva 2022).

¹⁴ For example, AASB (2019, p. 12); ASIC (sub. 2, p. 2); CA ANZ (2025, p. 3); CPA Australia (qr. 45, p. 3); EY Australia (qr. 27, p. 3).

Mandating digital financial reporting would also give report preparers and users the certainty they need to invest in the infrastructure and processes that enable productive exploitation of digital financial reports, overcoming the coordination issues that are discussed below. Key justifications for continuing with a voluntary submission scheme – that digital financial reporting will eventually be widely adopted under the existing voluntary scheme, that the advent of artificial intelligence (AI) and other digital technologies removes the need for digital financial reporting and that the costs associated with preparing digital financial reports are excessive – are flawed, particularly if an Australian mandate is designed with the experiences of other jurisdictions in mind.

Voluntary schemes do not encourage uptake

Australia will likely never realise the benefits of digital financial reporting if the existing voluntary submission scheme is maintained. The PC has identified several possible reasons why there has been no uptake of digital financial reporting under the voluntary system.

For report preparers, the anticipated costs of digital financial reporting have been raised as a barrier to adoption (although as box 4.6 outlines, these costs do not appear to be excessive). Upfront costs associated with software licences and staff training are estimated to be highest in the first year of preparing digital financial reports (Deloitte Access Economics 2023, pp. 28–29), and would add to preparers' existing reporting burden, which includes:

- the current requirement to submit financial reports in hard copy or PDF format (ASIC 2025a)
- numerous other corporate, tax, business activity, governance and social responsibility reporting requirements (Group of 100, sub. 1, pp. 4–6).

Accordingly, inquiry participants perceived 'time and effort', 'high implementation costs, and potential challenges around software availability and a shortage of qualified personnel' as barriers to preparing digital financial reports (CPA Australia, qr. 45, p. 4; The University of Sydney, qr. 21, p. 5).

There may also be non-tangible costs associated with digital financial reporting. For example, report preparers may feel that publishing more structured financial data limits their ability to construct a narrative around their financial results, and they may also be concerned about other entities being able to analyse their financial information more easily, particularly in competitive markets.¹⁵

These costs are a barrier to the uptake of digital financial reporting under a voluntary system because report preparers themselves may not receive significant benefits from digital reporting, particularly in the short term. Instead, as discussed above, the benefits of digital financial reporting accrue to a variety of report users. Thus, while digital financial reporting would deliver benefits to society overall, report preparers have limited incentives to shift to digital reporting.

Another reason for the lack of uptake could be the **coordination failures**¹⁶ associated with the transition to digital financial reporting. Specifically, one of the benefits of digital financial reporting for report preparers – cheaper and quicker access to data for performance benchmarking – can only be realised once a critical mass of preparers submit digital financial reports. Essentially, the value of digital financial reporting to each

¹⁵ As is the case with the preparer's financial statements, there are legal consequences if the surrounding narrative is materially false or misleading (Corporations Act, s. 1308).

¹⁶ Coordination failures occur where multiple parties could benefit from undertaking a particular action together but fail to do so. This creates a sub-optimal outcome for these parties, and for society more broadly.

report preparer (and to society as a whole) increases at an increasing rate as more preparers opt into it. As described by CA ANZ:

there is little incentive or value in an individual company voluntarily producing a digital report where others do not. (qr. 30, p. 3)

ASIC also identified a second coordination failure, between report preparers and report users.

ASIC's observation is that companies are not preparing digital financial reports – or, where they have prepared them, are not lodging them with ASIC – because investors and analysts are not set up to use them in Australia. However, analysts have not updated their systems because companies do not provide digital reports, leaving the uptake of voluntary digital financial reporting in Australia in a stalemate. (sub. 2, p. 2)

These market failures make it highly unlikely that there will ever be substantial uptake of digital financial reporting under the current voluntary regime. This is consistent with overseas experiences (box 4.4).

In their review of the literature relating to the adoption of digital financial reporting, Perdana et al. (2015, pp. 131–132) found that support from regulators and other government agencies was the most commonly identified factor driving uptake, and likewise, that a lack of support and pressure from government was the most common inhibitor. They asserted that the adoption of digital reporting is 'inextricably linked' with government policy, such as mandates (Perdana et al. 2015, p. 129).

Box 4.4 – Globally, voluntary reporting schemes have seen minimal uptake

Australia's voluntary approach to digital financial reporting makes us a global outlier. There are some other jurisdictions, however, that have chosen (or in most cases, temporarily attempted) to take a voluntary approach. As in Australia, these voluntary schemes have been plagued by persistently low uptake, with several being replaced by mandates over time.

- In **Canada**, uptake of voluntary digital financial reporting is higher than in Australia, but still negligible: in 2022, only 25 companies had submitted a digital financial report after more than a decade of it being possible to do so (Troshani and Rowbottom 2022, p. 7).
- When digital financial reporting was initially voluntary for listed companies in the **United States**, uptake was low, with only 2% of companies participating in the voluntary filing program. After three years of the voluntary scheme, the US SEC announced a staged transition to mandatory digital financial reporting (Chen 2010, p. 24).
- In **South Africa**, only one company had filed a digital financial report in the three years after the country's voluntary filing program was introduced in 2009 (Debreceeny et al. 2012, p. 51). Digital financial reporting was later mandated in 2018 (South African CIPC 2024).

In fact, in their response to Treasury's 2012 options paper on digital financial reporting, XBRL UK Jurisdiction (2013, p. 2) could only identify one successful large-scale voluntary scheme: the company accounts filing facility at UK Companies House. And that scheme cannot be considered purely voluntary, as it involves companies submitting digital reports to Companies House that are already being prepared under a mandate for His Majesty's Revenue and Customs, another government agency.

Technologies such as AI are a complement, not a substitute

The rapidly developing capabilities of AI and other digital technologies raises the possibility that they are adequate substitutes for digital financial reporting. These tools can make it more straightforward to *extract* information from non-digital financial reports. However, they are missing a key attribute of digital financial reports that is critical for conducting high-quality *analysis*: the structure of a taxonomy (IFRS Advisory Council 2022, p. 22).

Data needs to be structured before it is analysed – for example, before algorithms are run on it. Consequently, AI tools are inherently constrained in their capacity to analyse unstructured data that has been extracted from non-digital financial reports.

Under current policy settings, where reports are primarily submitted as non-digital PDF files, report users can use AI tools to extract and analyse financial information in different ways.

First, each report user could extract financial information from reports using AI, then manually assign their own taxonomy to the extracted data. This limits the quality of cross-report comparisons and restricts the extent to which analysis undertaken by different users can be compared. This situation is also duplicative, as it involves every user applying AI tools to independently create their own taxonomy when working with the same financial reports (IFRS Advisory Council 2022, p. 22).

Second, report users could also rely on AI tools to specify a taxonomy for the unstructured data that has been extracted from the non-digital PDF file. However, evidence suggests that AI tools are currently unable to consistently map financial information to a digital financial reporting taxonomy, and face particular difficulties when working with closely-aligned taxonomy items (Wang et al. 2025, p. 1). This poor performance manifests in absolute terms, as well as relative to the AI tools' capacity to extract data from financial reports: while the best-performing large language models extract data with an accuracy rate of about 70%, they map financial items to the correct item in a financial reporting taxonomy at less than 20% accuracy (Wang et al. 2025, p. 9).¹⁷ In contrast, when digital financial reports are prepared, the financial data is 'tagged' and structured within a nationally consistent taxonomy (box 4.2), ready to be analysed using AI tools.

Thus, while AI tools may be a reasonable substitute for digital financial reports when extracting data from non-digital financial reports, in the case of analysing data, having data structured within a taxonomy improves the ease and effectiveness with which algorithms, machine learning and other techniques can be applied.

Inquiry participants saw potential in using digital financial reports and technologies such as AI in a complementary way (box 4.5), and many inquiry participants recognised the need for AI tools to be underpinned by high-quality data.¹⁸

¹⁷ The evaluation metric used is an F1 score: a combination of precision (the rate at which identified items have been identified correctly) and recall (the rate at which all items that should have been identified have been identified) (Wang et al. 2025, p. 15).

¹⁸ ATN Universities (qr. 13, p. 3); Australian Information Industry Association (qr. 49, p. 6); CPA Australia (qr. 45, p. 6); EY Australia (qr. 27, p. 7); IoT Alliance Australia (qr. 8, p. 4); Marrickville Legal Centre (qr. 38, p. 4); Mauricio Marrone (qr. 28, p. 5); Salesforce (qr. 57, p. 5).

Box 4.5 – Inquiry participants envisaged using digital financial reports alongside AI

As structured formats ... become more widely adopted, the ability to harness AI in reviewing and comparing disclosures across companies will expand and offer tangible benefits to both institutional and retail investors. (Australian Shareholders' Association, sub. 44, p. 2)

[Digital financial reporting could] ... enable the use of advanced technology tools, such as AI, to more effectively identify trends or anomalies and generate deeper insights across large datasets, which in an audit sense could help drive the audit strategy and focus areas. (EY Australia, qr. 27, p. 3)

The main difference in the use of digital reports compared to other formats is that AI solutions work more effectively with digital reports. To date, we have found the use of AI to extract information from PDF financial reports to be unreliable. (The University of Sydney, qr. 21, p. 5)

For report preparers, there may be long-term cost savings

There are material costs associated with transitioning to digital financial reporting – report preparers anticipate needing to make 'upfront investment[s] in systems, processes, and staff training' (Group of 100, sub. 1, p. 2). However, there is evidence to suggest that over the longer term, the cost of digital reporting is comparatively lower than hard copy or PDF reporting.

Deloitte Access Economics estimated that an average large Australian company's first *digital* financial report submission would cost \$76,000, with subsequent submissions costing \$25,000 (2023, p. 29).¹⁹ In comparison, Treasury estimated that the average annual cost of preparing and auditing *non-digital* financial reports for large companies was about \$37,000 (2019).

In the United States, Harris and Morsfield (2012, p. 23) found similar short-term and long-term effects for report preparers: while most preparers considered the initial costs of digital financial reporting to be substantial, preparers also reported significant improvements in the efficiency of their reporting processes after moving 'beyond the initial implementation' period.

International evidence also indicates that the cost of digital financial reporting is not excessive and, in the case of the United States, is falling over time (box 4.6).

¹⁹ A company is 'large' if it meets at least two of three thresholds: consolidated revenue of \$50 million or more, consolidated gross assets of \$25 million or more and 100 or more employees (Treasury 2019).

Box 4.6 – International evidence indicates that the cost of preparing digital financial reports is not excessive

It is difficult to provide a single estimate of the costs associated with a transition to digital financial reporting for report preparers in Australia. This is because many factors influence the cost of digital financial reporting for each preparer, including:

- the number of data points within the report
- the size and industry of the report preparer
- the number of users of the software being used for digital report preparation
- the extent to which the preparation of digital reports is outsourced (US SEC 2024b, p. 6).

United States

In 2019, Nasdaq surveyed more than 100 listed companies about the cost of preparing digital financial reports. For these companies, the median cost was \$7,500 USD per quarter (Nasdaq 2019, p. 12). And in 2023, the US SEC estimated that smaller filers generally pay between \$1,500 USD and \$5,000 USD per year to prepare digital financial reports (either by outsourcing or preparing them in-house using appropriate software), while larger filers typically pay between \$5,000 USD and \$30,000 USD annually (US SEC 2024b, p. 6).^a Moreover, a 2018 study found that the average annual cost of preparing digital financial reports declined by 45% between 2014 and 2017 (AI CPA and XBRL International 2018, p. 1).

European Union

Prior to the introduction of mandatory digital financial reporting in the European Union, the European Securities and Markets Authority estimated the associated compliance costs for report preparers. The 2016 study found that for report preparers outsourcing the tagging process, their first submission was expected to cost EUR 8,200, with subsequent submissions costing EUR 2,400 (ESMA 2016, p. 64). For report preparers producing digital financial reports in-house, their first and subsequent submissions were estimated to cost EUR 13,000 and EUR 4,600, respectively (ESMA 2016, p. 65). More recently, German report preparers reported higher compliance costs of about EUR 18,000 annually (Accounting Standards Committee of Germany 2025, p. 23).

a. Smaller filers are entities with a public float of less than \$250 million or less than \$100 million in annual revenues (and either no public float or a public float of less than \$700 million) (US SEC 2024c).



Draft recommendation 4.1 **Make digital financial reporting the default**

The Australian Government should make the necessary amendments to the *Corporations Act 2001* (Cth) and the *Corporations Regulations 2001* (Cth) to make digital financial reporting mandatory for disclosing entities. The requirement for financial reports to be submitted in hard copy or PDF format should also be removed for those entities.

The PC is seeking feedback on implementation issues

What should the scope of a digital reporting mandate be?

Draft recommendation 4.1 is for digital financial reporting to be mandated for **disclosing entities**, including publicly listed companies and other public interest entities (box 4.1). The PC is seeking feedback on whether that is the right scope for the mandate. For example, the mandate could potentially be applied to a wider set of reporting entities, such as large proprietary companies.

The PC is also seeking feedback about whether a phased approach to implementation is needed, as suggested by some inquiry participants (EY Australia, qr. 27, p. 3; Group of 100, sub. 1, p. 3).

Draft recommendation 4.1 is about **financial** reporting. The PC is seeking feedback on whether a digital reporting mandate should be applied to other types of reporting, such as sustainability reporting. For example, report preparers in the European Union will soon be required to submit their sustainability reports in a digital format (EC 2025b, pp. 22–23).

What is needed to support high-quality financial data?

The PC is seeking feedback on whether there are any barriers that would prevent digital financial reporting from improving the quality and availability of financial data. Realising the benefits of digital financial reporting depends on how useful the reports are to users, and regulatory support for data quality has been important overseas (box 4.7). In particular, the PC is seeking feedback on whether Australia's digital reporting **taxonomy** and **regulatory requirements around reporting quality** are adequate to enable the preparation and submission of high-quality financial data.

Box 4.7 – Institutional support for data quality is important

While the first year of mandatory digital financial reporting in the United States was accompanied by significant concerns about data quality – one quarter of submissions in the first year of the mandatory scheme were found to have calculation errors (Debreceeny et al. 2010, p. 303) – over time, as report preparers have gained experience and software has been enhanced, reporting errors have fallen (Debreceeny et al. 2010, p. 297; Du et al. 2013, p. 63; Foshag 2025, p. 60).

In particular, there has been a steep decline in reporting errors since 2020 (Foshag 2025, p. 60). This has been attributed to the integration of a number of data quality rules^a within Electronic Data Gathering, Analysis and Retrieval (EDGAR), the submission portal for financial reports used in the United States (Foshag 2025, p. 20). Essentially, report preparers began receiving warning messages when data quality rules were not being met in their financial reports (Foshag 2025, p. 10). This is hypothesised to have not only improved report preparers' awareness of data quality rules, but also increased their capacity to detect and remediate errors before financial reports were submitted (Foshag 2025, p. 20).

a. Examples of data quality rules include that values that are part of an accounting constant should be consistent within a financial report (for example, Assets = Liabilities + Equity), and that dates associated with subsequent events or forecasts must be on or after the reporting period end date (XBRL US 2016, 2019).

Australia's digital financial reporting taxonomy

The preparation of digital financial reports relies on the existence of a taxonomy, a data dictionary of definitions and terminology used in financial reporting. Australia's business-to-government digital reporting taxonomy was created as part of the 2010 Standard Business Reporting reforms, and covers financial, prudential and taxation reporting. The taxonomy standardised commonly-used terms and definitions across approximately 400 government reports and reduced the number of unique data elements from more than 25,000 to about 6,000 (PC 2012, pp. 103, 111, 114).

ASIC has been updating the digital financial reporting taxonomy annually since it was made available in 2010. This taxonomy, referred to as the 'IFRS AU Taxonomy', is derived from the International Financial Reporting Standards (IFRS) Taxonomy, with some additional tags for Australia-specific disclosure requirements (ASIC 2025a).

Australia's digital financial reporting taxonomy should remain aligned with the IFRS taxonomy under a mandatory reporting scheme, as this would reduce compliance costs. This is because digital financial reporting in other jurisdictions – for example, foreign entities reporting to the US SEC – is in some cases based on IFRS taxonomies (US SEC 2024a).

The taxonomy must also be consistent with Australian Accounting Standards. While the Standards do not prescribe that financial reports are prepared in any particular format, the Corporations Act (s. 296(1)) does require that financial reports – and by extension, the taxonomy underlying them – be prepared in accordance with the Standards.

Regulatory requirements affecting quality

Australia's financial reporting legislative framework already contains regulatory requirements to ensure that submitted reports are of high quality. This includes requirements in relation to the accuracy of data, audit processes and compliance with accounting standards (box 4.1). The PC is seeking feedback on whether additional regulatory requirements or architecture are needed to deal specifically with the quality of digital financial reports. For example, the PC has identified two considerations.

- Report quality can be improved by using automatic **validation checks** when reports are submitted. For example, when submitting digital financial reports via the US SEC's EDGAR platform, report preparers receive error messages when required tags are missing, or where a negative value has been entered for a value that must be zero or positive (US SEC 2025).
- The use of **extensions** (where a report preparer tags data as belonging to an additional item that is not part of the defined taxonomy) provides report preparers with greater flexibility, but reduces the comparability of financial reports (Perdana et al. 2015, p. 134). Globally, requirements regarding extensions are varied, with different jurisdictions choosing to deny, restrict or enable preparers' use of extensions (Troshani and Rowbottom 2022, p. 12). Both the United States and United Kingdom have experienced issues with reports containing unnecessary extensions, where data has been tagged with an extension despite an appropriate tag existing in the taxonomy. This needlessly reduces the comparability of financial reports, although it does appear to be becoming less common over time (Hoitash et al. 2020, p. 16; UK FRC 2025).

What format should be adopted?

The PC is seeking feedback on whether there should be a prescribed format for digital financial reporting in Australia. Digital financial reports can be prepared in different formats, including as eXtensible Business Reporting Language (XBRL) or inline XBRL (iXBRL) files (Troshani and Rowbottom 2022, p. 5).

- In **XBRL** files, financial information appears in a code format (Troshani and Rowbottom 2022, p. 5). This means that the information can be read by machines (like computers) but must be translated into a different format (like an Excel file) before it is easily readable by humans.²⁰ In jurisdictions where digital financial reports have been submitted as XBRL files – such as the United States prior to 2018 – report preparers have also generally continued submitting additional non-digital, human-readable reports, such as HTML files (Hoitash et al. 2020, p. 14).
- In **iXBRL** files, the digital financial information is interactively embedded in a document that can be read like a standard document, so the reports are both human-readable and machine-readable (Troshani and Rowbottom 2022, p. 5). In several jurisdictions where digital financial reporting is mandatory – including the United States, United Kingdom, Japan and South Africa – reports must be submitted in iXBRL format (IFRS Foundation 2024, p. 5; South African CIPC 2024; UK FRC 2025; Wang et al. 2024, p. 2).

The key advantage of iXBRL files relative to XBRL is that they ‘cater to the needs of both humans and machines’ (Troshani and Rowbottom 2022, p. 17).

- **Report preparers** only need to prepare and submit a single financial report and can construct a narrative around their financial results as they do with non-digital financial reports.
- **Report users** wishing to utilise both the digital and non-digital information from a financial report only need to review a single file. Users who want to continue engaging only with non-digital information can also do so, as iXBRL files can be read like a standard document.
- For **regulators**, evidence from the United States indicated that the adoption of iXBRL reporting – relative to XBRL reporting – was associated with improved review efficiency by the US SEC, the nation’s corporate regulator. Wang et al. (2024, pp. 4–6) found that the US SEC was more likely to issue comment letters²¹ to entities that submitted iXBRL reports, particularly during busy periods. Relative to other comment letters, the comment letters sent to these entities also covered a broader range of topics and were produced in less time.

How should digital financial reports be submitted and accessed?

Submitting reports

When digital financial reporting was first made available in 2010, ASIC maintained an online submission portal. From 2020, given no entities had submitted digital financial reports and the costs involved in maintaining the portal, ASIC moved to accepting digital financial reports by email (ASIC, personal communication, 18 July 2025).²²

As a shift to mandatory digital financial reporting would involve a significant increase in the volume of digital financial reports received by ASIC and market operators, the PC is seeking feedback on how the reports should be submitted under a mandatory scheme.

²⁰ A human-readable version of an XBRL file will also only include raw financial information and will therefore not contain a narrative surrounding the financial results.

²¹ Comment letters are written feedback and guidance provided to entities after the US SEC has reviewed their filing (Wang et al. 2024, p. 1).

²² Non-digital financial reports are lodged via an online portal maintained by ASIC, or directly to a market operator (such as the Australian Securities Exchange) for publicly listed companies (ASIC 2018).

More uptake of, or mandating digital financial reporting would require the implementation of a new online lodgement portal. The rollout of multiple portals may also be preferred, as maintaining dual lodgement relief – where preparers that lodge financial reports with a market operator (such as the Australian Securities Exchange) do not also need to lodge financial reports with ASIC – would reduce publicly listed preparers' reporting burden. As discussed in the next section, an appropriately designed portal would also ensure that the digital financial reports are readily accessible to report users.

Accessing reports

Currently, financial reports are publicly available via ASIC for a fee (ASIC 2025b). Some companies also publish financial reports on their website.

The PC's present view is that it is important for digital financial reports to be both publicly and freely available. The site holding the reports should also have Application Programming Interfaces (APIs) that allow the reports to be downloaded. This is because realising the benefits of digital financial reporting hinges on financial information being easily accessible to report users (CA ANZ 2025, p. 21).

The Corporations (Fees) Regulations 2001 (Cth) (schedule 2, item 16) specifies the fee that ASIC must charge for document access. Providing a 'free access' portal where costs are not directly recovered via search fees would therefore require amendments to the regulations. The PC is seeking further feedback on this matter.

Are further steps needed to ease the reporting burden for preparers?

As discussed above, there will be costs associated with a transition to mandatory digital financial reporting, particularly for report preparers (box 4.6). Inquiry participants have suggested that appropriate lead times and support mechanisms – such as training programmes, guidance documentation and access to implementation specialists – would assist report preparers to transition to digital financial reporting (CPA Australia, qr. 45, p. 4; Group of 100, sub. 1, p. 3). It has also been suggested that there is scope to streamline other reporting requirements, which could further ease the reporting burden for report preparers (Group of 100, sub. 1, p. 3; Property Council of Australia, qr. 64, p. 3). The PC is seeking feedback on these issues.



Information request 4.1

The PC is seeking feedback on the implementation of mandatory digital financial reporting.

- Who should be required to submit digital financial reports? Should implementation be phased?
- Are there other reports that should be submitted digitally?
- What can be done to enable high-quality reporting and the production of high-quality data? For example, is the digital reporting taxonomy adequate?
- Should report preparers be required to prepare their digital financial reports in XBRL format, iXBRL format, either format or a different format?
- How should digital financial reports be submitted? How should they be made available to the public?
- What should be done to ease the reporting burden for preparers?

Appendices



A. Public consultation

This appendix outlines the consultation process and lists the organisations and individuals who participated in the inquiry. The PC received the terms of reference for this inquiry on 13 December 2024. The PC met with 84 individuals and organisations (table A.1). A consultation questionnaire was released on 19 May 2025 seeking feedback on specific aspects of our policy reform areas. In total, 75 responses to the questionnaire (table A.2) were received. An additional 46 submissions were received via email (table A.3). The questionnaire responses and submissions are available at: engage.pc.gov.au/projects/data-digital.

The PC would like to thank everyone who has participated in this inquiry.

Table A.1 – Consultations

Participants

Amazon AU
ARC Centre of Excellence for Automated Decision-Making and Society (ADM+S)
Associate Professor Katharine Kemp
Association for Data-driven Marketing and Advertising (ADMA)
Australian Banking Association (ABA)
Australian Communications and Media Authority (ACMA)
Australian Communications Consumer Action Network (ACCAN)
Australian Competition and Consumer Commission (ACCC)
Australian Computer Society (ACS)
Australian Copyright Council (ACC)
Australian Council of Trade Unions (ACTU)
Australian Financial Security Authority (AFSA)
Australian Government Attorney-General's Department (AGD)
Australian Government Department of Finance
Australian Government Department of Home Affairs
Australian Government Department of Industry, Science and Resources (DISR)
Australian Government Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts (DITRDCA)
Australian Government Treasury
Australian Information Industry Association (AIIA)
Australian Institute of Company Directors (AICD)
Australian Mobile Telecommunications Association (AMTA)

Participants

Australian Securities and Investments Commission (ASIC)

Australian Securities Exchange (ASX)

Australian Shareholders' Association (ASA)

Bill Hero

Biza.io

Bureau of Communications, Arts and Regional Research (BCARR)

Business Council of Australia (BCA)

Challenge Networks

Chartered Accountants Australia and New Zealand (CA ANZ)

CHOICE

Commonwealth Bank of Australia (CBA)

Communications Alliance

Connected Farms

Consentic

Consumer Policy Research Centre (CPRC)

Copyright Agency

Data Standards Body

Data Transfer Initiative (DTI)

Data61

Delia Rickard

Deloitte

Department for Business and Trade (United Kingdom)

Digital Industry Group Inc. (DIGI)

Dr Bill Roberts

Dr Ian Oppermann

Energy Flex

FinTech Australia

Glenn Cooper

Google Australia and New Zealand

Group of 100

Helios Salinger

Hon Dr Andrew Leigh MP

Honorary Associate Professor Glenn Archer

Inrupt

Jobs and Skills Australia (JSA)

Participants

Mastercard (Australasia)

Medical Software Industry Association (MSIA)

Meta

Microsoft

National Australia Bank (NAB)

National Farmers' Federation (NFF)

Nordic Institute for Interoperability Solutions (NIIS)

Office of the Australian Information Commissioner (OAIC)

Office of the National Data Commissioner (ONDC)

Open Banking Limited

OpenAI

Peter Harris

Philip Coppel KC

Professor Jeannie Paterson

Professor Joshua Gans

Professor Lauren Willis

Professor Nicole Gillespie and Dr Steve Lockey

QBE Insurance Group

Quantium

Rigby Cooke Lawyers

Solar Analytics

The Tech Council of Australia (TCA)

Therapeutic Goods Administration (TGA)

Vocus

WeMoney

Woolworths Group

XBRL International

Xero

Table A.2 – Questionnaire responses

Participants	qr no.
Aidan O'Shaughnessy	2
Atlassian Pty Ltd	50
ATN Universities	13
Australasian Performing Right Association Ltd (APRA AMCOS)	58
Australian Copyright Council (ACC)	72
Australian Digital Health Agency	16
Australian Industry Group (Ai Group)	48
Australian Information Industry Association (AIIA)	49
Australian Production Design Guild (APDG)	6
Australian Publishers Association & Australian Society of Authors	39
Australian Recording Industry Association of Australia (ARIA) and the Phonographic Performance Company of Australia Ltd (PPCA)	65
Australian Retail Credit Association (Arca)	61
Australian Smart Communities Association (ASCA)	14
Australian Writers' Guild, Australian Writers' Guild Authorship Collecting Society, Australian Guild of Screen Composers, Australian Screen Editors, Australian Screen Directors Authorship Collecting Society & Australian Directors' Guild	12
Business Software Alliance (BSA)	73
Cancer Council Australia	11
Chartered Accountants Australia and New Zealand (CA ANZ)	30
Chegg	25
Copyright Agency	7
CPA Australia	45
Creative Australia	62
David Hardidge	19
Digital Health Cooperative Research Centre (DHCRC)	74, 75
Engineers Australia	59
EY Australia	27
FinTech Australia	66
Frollo Australia Pty Ltd	55
Global Shield Australia	46
Good Ancestors Policy	5
GS1 Australia	63
Heavy Vehicle Industry Australia (HVIA)	20

Participants	qr no.
Insurance Council of Australia (ICA)	29
Intuit Australia	36
IoT Alliance Australia	8
KPMG Australia	60
Lee Reynolds	4
Maritime Union of Australia (MUA)	71
Marrickville Legal Centre	38
Master Electricians Australia (MEA)	51
Mauricio Marrone	28
Medical Software Industry Association (MSIA)	70
Microsoft	52
Moir Scerri	53
Montu Group Pty Ltd	35
Mortgage & Finance Association of Australia (MFAA)	67
Murdoch Children's Research Institute (MCRI)	34
Myna Group	54
MYOB	31
National Growth Areas Alliance (NGAA)	43
Ojasvi Rana	68
Property Council of Australia	64
Regional Universities Network (RUN)	22
Roche Diagnostics	33
Salesforce	57
Schools Copyright Advisory Group (CAG Schools)	40
Screenrights	17
Social Ventures Australia (SVA)	26
Super Members Council (SMC)	37
TAFE Copyright Advisory Group (CAG TAFE)	41
Tax Justice Network Australia	42
The George Institute for Global Health	32
The Tech Council of Australia (TCA)	69
The University of Sydney	21
Uniting Church in Australia, Synod of Victoria and Tasmania	44
Visa	24
Workday Australia	56

Participants	qr no.
Xero	18
Anonymous	1
Anonymous	3
Anonymous	9
Anonymous	10
Anonymous	15
Anonymous	23
Anonymous	47

Table A.3 – Submissions

Participants	Sub no.
Amazon AU	33
ARC Centre of Excellence for Automated Decision-Making and Society (ADM+S)	14
Association for Data-driven Marketing and Advertising (ADMA)	46
Australian Academy of Science (AAS)	38
Australian Academy of Technological Sciences & Engineering (ATSE)	12
Australian Chamber of Commerce and Industry (ACCI)	19
Australian Communications Consumer Action Network (ACCAN)	37
Australian Council of Trade Unions (ACTU)	31
Australian Film/TV Bodies	40
Australian Financial Markets Association (AFMA)	27
Australian Information Industry Association (AIIA)	4
Australian Institute of Company Directors (AICD)	18
Australian Retailers Association and National Retail Association	21
Australian Securities and Investments Commission (ASIC)	2
Australian Shareholders' Association (ASA)	44
Australian Small Business and Family Enterprise Ombudsman (ASBFEO)	43
Bunnings Group	22
Business Council of Australia (BCA)	16
Chamber of Commerce and Industry Western Australia (CCIWA)	25
Civil Contractors Federation Australia Ltd (CCF)	8
Coca-Cola System	17
Commonwealth Bank of Australia (CBA)	35
Council of Small Business Organisations Australia (COSBOA)	30

Participants	Sub no.
Digital Economy Council of Australia (DECA)	15
Digital Industry Group Inc. (DIGI)	42
Free TV	10
Google Australia and New Zealand	32
Governance Institute of Australia Ltd	28
Group of 100	1
Group of Eight Australia (Go8)	41
GS1 Australia	9
Heavy Vehicle Industry Australia (HVIA)	6
HumanAbility	3
Lite n Easy	5
Master Builders Australia	34
Mastercard (Australasia)	26
Maurice Blackburn	24
Meta	39
National Electrical and Communications Association (NECA)	11
NewDirection Care	20
Regional Australia Institute (RAI)	13
Screen Producers Australia (SPA)	45
Telstra	36
The Pharmacy Guild of Australia	29
The Smith Family	23
Woolworths Group	7

B. Modelling the benefits of data and digital reforms

B.1 Summary

Every year, more data is produced (PM&C 2021, p. 11), more goods and services move online (ABS 2024d, table 23) and new technologies like artificial intelligence (AI) offer new opportunities to leverage data. It follows that the free flow of data will likely be an important driver of growth in the Australian economy. In this context, this appendix attempts to quantify the potential contribution to economic growth of the policy reforms considered in this report.

The Productivity Commission has produced three quantitative indicators that contextualise potential reform benefits. These are subject to significant uncertainty, and we welcome feedback – including about data and methodology – that could be used to refine and improve these estimates.

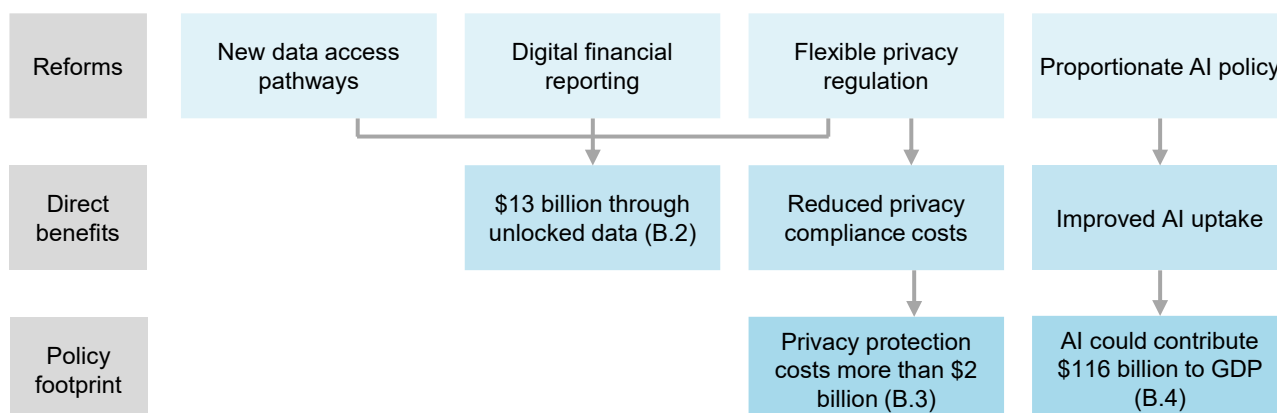
Improved use of data (section B.2). Within the next decade, unlocking data through new regulatory pathways for data access, outcomes-based privacy regulation and digital financial reporting (chapters 2 to 4) may yield benefits on the order of a 0.5% increase in whole economy labour productivity, or \$13 billion annually. Beyond the next decade, productivity gains may be even greater due to higher innovation and increasing digitisation.

Reduced privacy compliance burden (section B.3). Under the status quo, an estimated 10,000 firms with turnover of at least \$50 million are affected by the *Privacy Act 1988* (Cth). Collectively, direct ongoing expenditure on privacy could be on the order of \$2 billion, with additional one-off and indirect costs. The Privacy Act also affects an estimated 267,000 smaller firms, however, costs for individual firms are unknown, and hence we have not produced a cost estimate.

Artificial intelligence (section B.4). Estimates suggest that AI could improve multifactor productivity by 0.5% to 13% over the next decade, although the PC considers gains of at least 2.3% likely. This could translate to an additional 4.3% labour productivity, contributing \$116 billion to GDP.

These indicators have different scopes (figure B.1). While the PC has estimated direct reform benefits arising from improved use of data, the PC has not been able to directly estimate the impacts of privacy or AI reforms. Instead, the PC has considered the productivity impacts of the Privacy Act and AI, which are useful benchmarks for understanding potential reform impacts.

Figure B.1 – Significant opportunities are available



B.2 Improved use of data

Reforms that improve access to data, reduce the burden of privacy regulation and mandate digital financial reporting will help unlock Australian data and boost productivity.

- *New regulatory pathways for data access* can drive the creation of more personalised and effective products and services, spurring competition and innovation.
- *Privacy regulation* that gives firms more options about how they achieve privacy outcomes can facilitate innovative uses for data where current privacy regulations make it unnecessarily difficult to share and use data.
- *Digital financial reporting* increases the efficiency, transparency and accuracy with which data in financial reports is prepared, extracted and analysed.

Estimated gains from data vary heavily based on methodology

Taking a growth accounting approach implies benefits below 0.5% of GDP. Smedes et al. (2022, table 3) estimated that data production and analysis were worth 8.5% to 11.1% of investment in 2016. If data contributes about 10% to capital services (that is, assuming data's 10% share of investment corresponds to 10% of capital services flows),²³ then a growth accounting framework might imply that a (relatively high) 10% increase in the value generated by data would be required for about a 0.5% increase in aggregate productivity.²⁴ However, such an approach might not account for particularly valuable uses for data.

Examining potential uses for data implies benefits worth at least 1% of GDP. An OECD (2019, p. 60) literature review found benefits from public and private sector data access and sharing worth 1% to 2.5% of GDP (with a few studies as high as 4%), while Lateral Economics (2014, p. x) estimated that reinvigorated open data policies could contribute about 1% to Australian GDP. For specific data uses, White et al. (2021, p. 10) estimated a 1 to 1.5% increase in GDP from open financial data (for the United Kingdom, United

²³ Capital services refer to the flow of services (value) from capital. Ideally, capital services would be calculated based on the capital stock associated with data, but Smedes et al.'s (2022) estimates of the capital stock related to data were very sensitive to the assumed asset life of capital and the assumed rate of cost inflation. Instead, the share of investment may be a rough proxy for the share of capital services, although data investment may have increased by a percentage point or two since 2016 (data had already grown from 7.0% to 9.1% of investment in 2011).

²⁴ A 10% increase in the value generated by data would equal a 1% increase in capital services (as 10% of capital services would increase by 10%). With a 47% capital share of output (ABS 2025d, table 2) this would produce a 0.5% increase in output ($\% \Delta \text{output} = \% \Delta \text{productivity} + 0.53 \times \% \Delta \text{labour} + 0.47 \times \% \Delta \text{capital}$ and hence $0.47 \times 1\% = 0.47\%$).

States and European Union) and Deloitte Access Economics (2023, p. 14) estimated a \$6 billion increase in GDP (0.2% of 2024 GDP; ABS 2025b, table 1) from the digital financial reporting data of large Australian companies.²⁵

These types of benefit estimates are highly dependent on the details of each policy, and the costs of implementing that policy – which can be sizeable. For example, costs to implement the Consumer Data Right in Australia exceeded expectations, with large data holders reporting costs above \$100 million each (Treasury 2023b, p. 2).

There are reasons to think the total social value of data is greater than its private value. Data is non-rival and can be used to improve decision making. This results in increasing social returns to scale (Jones and Tonetti 2020) and hence the social value generated by data may exceed its private cost²⁶ (OECD 2022b, p. 15). For instance, small changes in financial data access arrangements can have significant effects on access to capital (Li et al. 2012) and productivity (Liu and Zhang 2024). Similarly, data from the Australian Census improves government decision making, resulting in \$6 of returns for every \$1 of costs (Lateral Economics 2019, p. 9).

Reform benefits may be on the order of a 0.5% increase in productivity within the next decade and will continue to grow

Over the next decade, the PC considers a 0.5% increase in labour productivity (worth \$13 billion relative to Australia's \$2.67 trillion 2023-24 GDP; ABS 2025b) to be indicative of reform benefits. These benefits are a midpoint between a more conservative growth accounting approach and more optimistic estimates based on the value of data. Apportioning these benefits may imply gains on the order of \$1 to \$10 billion per reform.²⁷

While these estimates are subject to significant uncertainty, examples of reforms and reform proposals concerning data policy show the benefits can be significant.

- *New regulatory pathways for data access* would involve a suite of targeted reforms and sharing initiatives. To take one example, electronic medical records could save \$5 billion per year by reducing the length of time patients spend in hospital (PC 2024b). While some benefits may be offset by implementation costs, large opportunities are available.
- *Privacy regulation* can have a substantial effect on technology and data firms. For instance, the EU General Data Protection Right imposed substantial costs on these firms, leading to EU technology venture investment falling by 24% relative to the US (Jia et al. 2021, p. 4) and entry of apps into the global market falling by half (Janssen et al. 2022). By moving to an outcomes-based approach to privacy regulation, Australia can avoid such costs and enable firm data use, on which the delivery of services to consumers is based.
- Deloitte Access Economics (2023, p. 14) modelling suggested the benefits from the *digital financial report* data of large Australian companies²⁸ may add \$6 billion to GDP (non-data related benefits could add an additional \$1.7 billion).³

²⁵ Total modelled benefits were \$7.7 billion. 78% were due to data access: 74% because the cost of capital falls when financial analysts get better data access and 4% from efficiency gains to auditors and regulators. 22% were not attributable to data access and were mostly due to easier preparation of financial reports.

²⁶ The total social costs of data may also exceed its total social benefits in certain scenarios, such as where there are significant impacts on privacy.

²⁷ For instance, if each reform contributes 10% to 75% of total benefits.

²⁸ The benefits were modelled based on a digital financial reporting mandate being applied to all Australian businesses with more than \$50 million in annual revenue, one of the three thresholds that defines a 'large company', with large companies needing to meet two of these three thresholds (Deloitte Access Economics 2023, p. 28; Treasury 2019).

In the long run, greater benefits may accrue where data unlocks additional innovation. Data directly contributes to research and innovation (PC 2017, pp. 108, 115–116), but data access also indirectly boosts innovation through access to credit²⁹ and increased competition (OECD 2021b).

B.3 Reducing privacy compliance burdens

The Privacy Act imposes two main costs: compliance costs and opportunity costs (which include reduced use of data). Compliance costs consist of the activities firms undertake to fulfil their regulatory obligations. For instance, hiring lawyers to help understand regulation, managing responsibilities through internal processes or building privacy compliant products. Opportunity costs refer to forgone benefits, such as where regulations prevent the use of data or creation of innovative products. Reforms may be able to reduce both these costs without reducing privacy protections where regulatory flexibility is improved.

A conservative estimate of compliance costs is about \$2 billion annually but costs could be many billions higher. These costs are for the approximately 10,000 firms holding personal information with turnover of at least \$50 million (large firms may be most able to utilise outcomes-based regulatory pathways) and may exclude one-off costs, second order distortions and be vulnerable to some underreporting bias. Costs for the 267,000 smaller firms also affected by the Act (that is, firms with Privacy Act responsibilities but less than \$50 million in turnover) are also likely significant.

The PC has not estimated opportunity costs directly resulting from the Privacy Act. However, the value of data unlocked through privacy reforms may be on the order of \$1 to \$10 billion (section B.2). Nonetheless, this figure only covers opportunity costs relating to the use of data.

Measured privacy protection costs

Methodology

The Privacy Act predominately covers large firms (OAIC 2023b). While most small businesses are exempt (where turnover is less than \$3 million), small businesses in some sectors are still covered. For instance, private sector health service providers (including medical practitioners, gyms, childcare centres and private educational institutions), credit reporting bodies, contracted service providers for the Australian Government and employee associations are all covered. For large organisations, certain exemptions may also apply, such as for state and territory governments, political parties, public universities except the Australian National University, public schools and media organisations.

To estimate the number of affected businesses, the PC sourced data from the Counts of Australian Businesses and the Business Longitudinal Analysis Data Environment (BLADE). BLADE was preferred for businesses with turnover of at least \$3 million due to the improved granularity of data, while the Counts of Australian Businesses was used for smaller firms as it is a public, ABS-vetted data source. Firm counts were then multiplied by the assumed number of firms holding personal information, which was extrapolated to Australia from the UK Business Data Survey, because such information is not available in Australia.

²⁹ 19% of Australian businesses reported lack of access to funds as a barrier to innovation (ABS 2024a, table 2). Data access arrangements can improve access to credit (White et al. 2021, p. 6).

Costs for large firms were sourced from IAPP and EY (2022), an international survey of privacy professionals. These costs were converted to AUD, inflated to 2023-24 dollars and then scaled down by a factor of five³⁰ to account for the fact that the IAPP-EY sample was focused on privacy active firms.³¹

Findings

These estimates imply a cost on the order of \$2 billion annually for the estimated 10,000 businesses³² with turnover of at least \$50 million who hold personal information (table B.1). But this estimate is imprecise. The proportion of firms holding data is drawn from the United Kingdom and costs are from overseas privacy-active firms (but are scaled down to reflect all Australian firms holding data). However, it is unlikely that the average large data holding Australian firm spends more on privacy than the average privacy intensive firm worldwide. Under this assumption, \$9 billion³³ seems like a reasonable upper bound for privacy expenditure. While 10,000 is a small proportion of the firms covered, these firms account for a sizeable proportion of economic activity.³⁴

Limited evidence is available for the costs among the estimated 267,000 businesses³⁵ with turnover below \$50 million who are affected by the Privacy Act. PC calculations based on IAPP and EY (2022, p. 46) suggest large economies of scale for privacy expenditures, with the largest firms (revenue at least US\$20 billion) spending less than 0.02% of revenue and the smallest (revenue less than US\$100 million) spending at least 0.5% of revenue. However, smaller firms are less likely to hold data (DSIT 2024) and may be less privacy mature (Helios Salinger 2025, p. 7) resulting in lower expenditure.

³⁰ While the choice of a scaling factor was somewhat arbitrary, scaled results represent an order of magnitude for measured costs. Unscaled costs represent an upper bound for measured costs.

³¹ The IAPP-EY sample was drawn from privacy compliance professionals, meaning it was focused on firms where privacy costs were likely disproportionately high.

³² 6,303 + 3,108 + 679 (table B.1).

³³ Multiplying unscaled costs from IAPP and EY (2022) by the count of firms equals \$9 billion. This is a reasonable upper bound as it is likely that the largest bias affecting this number is the privacy intensive nature of the sample, leading to an overestimation of costs.

³⁴ The total income across businesses in 2023-24 was \$5.3 trillion (ABS 2025a, table 1), while multiplying out the lower bound turnovers by the count of firms with at least \$50 million in turnover holding data in table B.1 implies at least \$1.46 trillion, or at least 28%.

³⁵ 159,000 + 107,575 (table B.1).

Table B.1 – Compliance costs for the largest firms may be on the order of \$2B annually
Privacy cost estimates for firms by size, 2023-24

	Potentially covered businesses ^a	Businesses holding personal information ^b	Cost per business ^c	Total cost
<\$3M ^d	177,000	159,000	Unknown	Unknown
\$3M to <\$50M	134,469	107,575	Unknown	Unknown
\$50M to <\$150M	7,003	6,303	\$150,000	\$945M
\$150M to <\$1B	3,453	3,108	\$170,000	\$528M
At least \$1B	754	679	\$500,000	\$340M
Total	322,679	276,965		>\$1.8B

a. Businesses include companies, partnerships, sole traders and trusts. **b.** In the United Kingdom, 56% of businesses with no employees, 62% of those with 1 to 9, 79% of those with 10 to 49, 88% of those with 50 to 249 and 90% of those with 250+ held digitised non-employee personal information. On the basis that few large businesses would hold personal information but no digitised records, it was assumed that 90% of Australian businesses with turnover at least \$50 million and 80% of those with turnover at least \$3 million but less than \$50 million held personal information. **c.** Costs were roughly matched by firm size, converted from USD to AUD using 2022 PPPs, inflated to 2023-24 dollars and then divided by five to account for sampling bias. **d.** For businesses with turnover less than \$3 million, only hospitals, medical and other health care services, residential care services, childcare services and credit reporting services were considered. At the end of 2023-24, there were 173,000 of these businesses with turnover below \$2 million and 7,000 with turnover at least \$2 million but less than \$5 million of which 53% (based on BLADE statistics for businesses in all industries) were assumed to have turnover below \$3 million. It was assumed that 90% of these businesses held some personal information as most would be customer facing or interact with medical records (in the United Kingdom only 69% of human, health and social work businesses held digitised personal information, but many of the remaining 31% may have held non-digitised personal information).

Source: PC calculations based on ABS (2024c, 2024b, 2025c), DSIT (2024), World Bank (2025).

Bias and underestimation

Limitations suggest that the total burden of privacy regulation may be somewhat higher.

- **One-off costs.** IAPP and EY (2022) asked privacy professionals for the annual costs of their organisations' privacy programs. This could omit the costs to setup or modify privacy programs which may be significant, although incurred infrequently. For instance, cost of the transition to the EU's General Data Protection Regulation was well above the ongoing privacy budget of organisations (PC calculations based on IAPP and EY 2017, pp. 21, 50, 2018, pp. 41, 80).
- **Self-reporting bias.** Survey respondents may underestimate costs. For instance, a respondent in the privacy department may not have oversight over privacy costs incurred by other departments.
- **Second-order distortions.** Costs were proportionally higher for smaller firms, potentially contributing to competition distortions. In addition, the Privacy Act threshold of \$3 million turnover might discourage small firms from expanding.

B.4 Estimating the productivity effects of AI

Previous studies have predicted that AI will raise multifactor productivity (MFP) by 0.5% to 13% over the next decade. After examining the evidence presented in these studies, the PC considers that gains of at least 2.3% are likely over the next decade, which would correspond to a 4.3% increase in labour productivity worth an additional \$116 billion in GDP. While the potential gains from AI are significant, some of them are likely to be mismeasured and not fully reflected in economic statistics.

Studies forecast 0.5% to 13% multifactor productivity growth over the next decade due to AI ...

A common way to estimate the short- to medium-term gains from AI is to consider the impact on *existing* economic activities ('task-based estimates'). This can be achieved by multiplying the share of tasks to which AI will contribute, by the average productivity improvement per task (Acemoglu 2025). Such estimates exclude second- or third-order effects as the economy adjusts to AI.

Task-based estimates range from 0.53% to 6.8% multifactor productivity improvement across the next decade (table B.2). Conservatively, Acemoglu (2025) estimated a 0.53% productivity improvement based on 20% of tasks being potentially exposed and AI being adopted for 23% of these tasks, with an average 11.5% efficiency gain. More optimistically, Aghion and Bunel's (2024) task-based estimate was 6.8%.

Alternative approaches estimate gains as high as 13%. Aghion and Bunel (2024) also compared AI to past technological revolutions, estimating 8% to 13% multifactor productivity gains. Briggs and Kodnani (2023) examined direct labour cost savings and effects on displaced and non-displaced workers, estimating a 15% increase in labour productivity. However, multifactor productivity gains may be only about half (Acemoglu 2025, p. 46) to two thirds (Filippucci et al. 2025, p. 21) as high as labour productivity gains.

Table B.2 – AI may increase productivity by several percentage points^a
Multifactor productivity (or labour productivity as indicated) improvement due to AI over the next decade

	Productivity ^b	Region ^c	Methodology
Acemoglu (2025)	0.53%	US	Task-based: 4.6% of activity improved by 11.5%
Aghion and Bunel (2024)	6.8% (0.7–12.4%)	US	Task-based: 30% of activity improved by 22.8%
Bergeaud (2024)	2.9% (1.3–4.5%)	EU	Task-based: 17.2% of activity improved by 16.8%
Briggs and Kodnani (2023)	15% (3–30%) labour productivity	US	Based on direct labour cost savings, a productivity boost for non-displaced workers and a composition effect from displaced worker reemployment
Chui et al. (2023)	3–7% labour productivity	US	Based on projected benefits across a set of industry use cases
Filippucci et al. (2025)	5.7% (2.3–7.5%)	Canada	Task-based: 19% of activity improved by 30%
Misch et al. (2025)	1.1% ^d	EU	Task-based estimate

a. The PC has recalculated effects from some papers to enable comparisons. For instance, growth rates from Aghion and Bunel (2024), Briggs and Kodnani (2023), Chui et al. (2023) and Filippucci et al. (2025) have been multiplied by ten to calculate the effect over the next decade (this approximation is consistent with Aghion and Bunel 2024). Additionally, some numbers in the methodology column were interpolated for Acemoglu (2025), Aghion and Bunel (2024), Bergeaud (2024) and Filippucci et al. (2025). **b.** Confidence intervals are displayed in brackets where available. **c.** AI gains tend to accrue more in higher-income economies (Chui et al. 2023, p. 45; Misch et al. 2025) but will also be affected by factors such as sectoral composition and the pace of AI adoption (Filippucci et al. 2025, p. 24). **d.** Misch et al. (2025, p. 7) expected medium run gains to occur within five years, rather than ten.

... but the lower end of this interval seems pessimistic

The PC reviewed the estimate of Acemoglu (2025), finding that Acemoglu may understate the benefits arising from falling compute costs, AI-as-a-service models and capital savings. Revising Acemoglu's

estimate after accounting for these factors implies gains of 2.3%. When considering the revised estimate and the higher estimates presented by other studies,³⁶ gains of at least 2.3% appear likely. However, these gains are not guaranteed due to the considerable uncertainty involved in any forecast.

Following Acemoglu (2025), the PC used Hulten's theorem: total multifactor productivity gains equal the proportion of the economy affected times the gains in affected areas. Acemoglu expects AI to increase the efficiency of 4.6% of economic activity by 11.5% (equation 1).

$$\Delta \text{MFP}_{\text{Acemoglu}} (0.53\%) = \text{share of economic activity} (4.6\%) \times \Delta \text{MFP in affected areas} (11.5\%) \quad (1)$$

PC estimates (equation 2) depart from Acemoglu in two regards.

- Acemoglu estimated that AI will only be used for 4.6% of tasks, due to low profitability. Based on rapidly falling compute costs and the potential for AI-as-a-service models, the PC estimates that AI will be adopted for 14% of tasks.
- Acemoglu assumed that AI would only increase the labour output, estimating an 11.5% productivity gain for affected tasks. Based on AI's potential to increase the output of both labour and capital, the PC estimated a 16.4% multifactor productivity gain.

$$\Delta \text{MFP}_{\text{PC}} (2.3\%) = \text{share of economic activity} (14\%) \times \Delta \text{MFP in affected areas} (16.4\%) \quad (2)$$

More detail on each assumption is provided below.

Proportion of economic activity affected by AI

Acemoglu (2025) estimates that AI will be used for 4.6% of tasks based on 20% of tasks being potentially exposed to AI and AI use being profitable for 23% of these tasks. That is:

$$\text{share of economic activity}_{\text{Acemoglu}} (4.6\%) = \text{share of tasks exposed} (20\%) \times \text{adoption rate} (23\%) \quad (3)$$

The estimate of exposed tasks draws on Eloundou et al.'s (2024) estimates of exposure to large language models (LLMs) and computer vision. The proportion of tasks that could be profitably automated ('adoption rate') is based on Svanberg et al. (2024), who examined the share of computer vision tasks that could be profitably automated at the firm level given 2022 compute prices.

The PC retains Acemoglu's 20% task exposure but assumes that AI use will be profitable in 70% of scenarios. This figure is chosen for three reasons.

- Compute costs have been falling rapidly. Aghion and Bunel (2024, pp. 7–9) find that rapidly falling AI compute costs of about 22% per year imply that 50% of computer vision tasks will be profitable to automate in the next decade.
- Each firm does not have to build their own solution. Svanberg et al. (2024, p. 19) find that adoption was profitable for 88% of tasks, if a single solution could be rolled out across the US.
- Computer vision may be a poor comparison for LLMs and other AI use cases. Svanberg et al. (2024) focus on automating specific tasks, but tools like LLMs may be able to support workers across different contexts, driving down unit costs.

As such, the PC assumed that half of adoption would involve custom firm level solutions, and the other half would relate to prebuilt cross-firm solutions. For custom, firm-level solutions, 50% were estimated to be

³⁶ Misch et al. (2025) also follows Acemoglu's approach with a relatively low estimate for the productivity effect of AI, albeit over a shorter time span (1.1% over 5 years for the EU). However, Misch et al.'s result depends on assumptions shared with Acemoglu. Most notably, Misch uses the adoption rate of Svanberg et al. (2024) (23%). So, the below discussion that suggests alternatives to Acemoglu's assumptions also apply to Misch et al.'s estimate.

profitable in line with Aghion and Bunel (2024). For a single ‘prebuilt’ cross-firm solution, Svanberg et al. (2024) found 88% of exposed tasks profitable at 2022 prices, so 90% is a conservative estimate as compute costs fall. This implies adoption of AI for at least 14% of tasks (equation 4).

$$\text{share of economic activity}_{\text{PC}} (14\%) = \text{share of tasks exposed} (20\%) \times \text{adoption rate} \left(\frac{50\% + 90\%}{2} \right) \quad (4)$$

This estimate is conservative when focusing on LLMs. LLMs like Copilot, ChatGPT and Gemini are largely being developed by a small set of big firms and then licensed out. Even where firm level solutions are used, they may be built upon existing systems. These LLMs can be used across tasks so are likely to be cost effective in most scenarios. For instance, premium access to LLM chatbots only costs around \$40 a month (OpenAI 2025b; RBA 2025), but every 1% increase in labour productivity for the average Australian worker yields \$150 a month (PC calculations based on ABS 2025e, table 1, 2025b, table 1).

Productivity gain for affected tasks

Acemoglu (2025, pp. 43–45) estimated an 11.5% multifactor productivity increase for affected tasks. This was based on 27% labour savings sourced from Brynjolfsson et al. (2025) and Noy and Zhang (2023). Acemoglu then adjusted this downwards to account for difficult tasks, estimating 21.5% labour savings based on 27% labour savings for the 72.6% of tasks that are easy and 7% labour savings for the 27.4% of tasks that are hard. Finally, Acemoglu converted these labour savings to multifactor productivity by multiplying them by the labour share of output for affected US industries (53.5%).³⁷ That is:

$$\Delta \text{MFP in affected areas}_{\text{Acemoglu}} (11.5\%) = \text{labour share of income in affected occupations} (53.5\%) \times \text{task labour saving} (21.5\%) \quad (5)$$

The PC considers 21.5% labour savings as a conservative but reasonable estimate. Filippucci et al. (2025, p. 10) consider a broader set of studies and come to a similar conclusion before accounting for hard tasks like Acemoglu (2025). However, it is worth noting that most task-level evidence comes from earlier AI models and gains are increasing as AI rapidly develops. For instance, Schwarcz et al. (2025), found that unlike earlier models, new retrieval augmented generation and reasoning models could improve work quality for complex legal tasks.

However, in line with Filippucci et al. (2025, p. 9) the PC does not consider gains to be purely labour saving.

- Purely *labour-saving gains* save on labour costs, but not capital. For instance, automation in a factory means less workers can produce the same amount with the same amount of capital. Hypothetically, eight workers and one factory instead of ten workers and one factory could now maintain a set level of output.
- *Labour and capital-saving gains* directly increase productivity. For instance, an LLM may increase the output of a programmer *and* their associated capital (laptop, office space). Hypothetically, eight programmers, eight laptops and 80% of an office could now produce what previously took ten programmers, ten laptops and an entire office.

In the context of AI and especially LLMs, the PC considers that labour and capital saving gains are more likely. For instance, AI is likely to directly increase productivity for knowledge work like programming. As a conservative middle-ground, the PC assumes that half of use cases will directly increase productivity, and

³⁷ This explanation rearranges Acemoglu’s calculations for consistency with our approach. Acemoglu calculated multifactor productivity separately for hard and easy tasks (14.4% and 3.7%), but 11.5% is the weighted average of these.

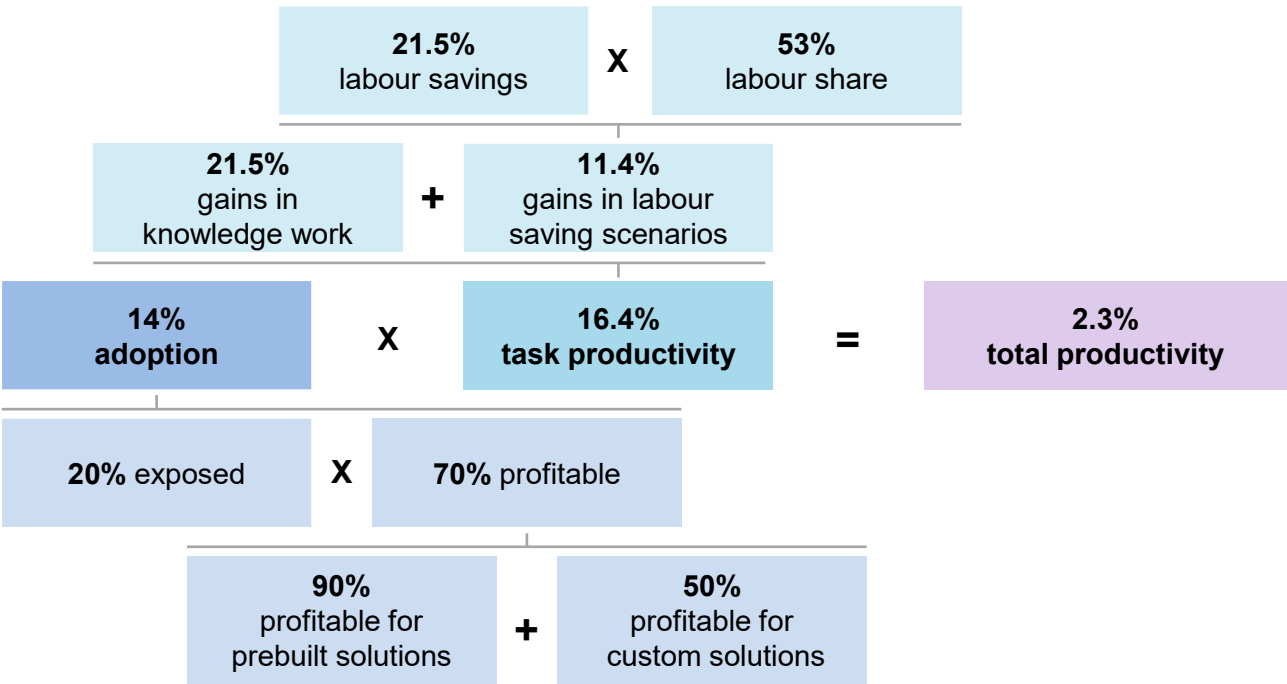
half will only reduce labour costs. Given the 53% labour share in Australia (ABS 2025d),³⁸ this implies 16.4% gains in multifactor productivity.

$$\begin{aligned} \Delta \text{MFP in affected areas}_{\text{PC}} (16.4\%) &= \frac{1}{2} \text{labour share of income in affected occupations (53\%)} \\ &\quad \times \text{task labour saving (21.5\%)} \\ &\quad + \frac{1}{2} \text{task joint labour and capital savings (21.5\%)} \end{aligned} \tag{6}$$

Revised task-based estimate

Based on these assumptions, the PC estimates a task-based multifactor productivity gain of 2.3% (figure B.2). While there is uncertainty involved in any projection, 2.3% gains are still more conservative than most other projections and compare well with other benchmarks (table B.2). For example, US survey evidence suggests AI may already be offering time savings amounting to 1.4% of work hours (Bick et al. 2024).

Figure B.2 – AI is likely to contribute at least 2.3% to multifactor productivity^a
Assumptions underpinning PC’s conservative estimate of AI’s productivity dividend



a. Numbers may not sum due to rounding. Gains in labour saving scenarios were lower than Acemoglu (2025) due to differences in the labour share.

³⁸ Ideally, estimates would be based on the labour share of income in affected occupations rather than across all occupations. However, Acemoglu uses a very similar labour share after making this adjustment (53.5%) for the US and very minor differences are unlikely to substantially affect results.

Multifactor productivity gains above 2.3% over the next decade due to AI seem likely

Excluding the Acemoglu paper, which as discussed above seems overly pessimistic, most other studies estimate much larger multifactor productivity gains accruing from AI (excluding Misch et al., footnote 13). Considering just these studies, AI seems likely to produce multifactor productivity gains above 2.3% over the next decade.

2.3% multifactor productivity would mean higher output and higher living standards. Using Acemoglu's (2025, pp. 33–34) approximation implies a 4.3% increase in labour productivity (ABS 2025d, table 2; equation 7). This would correspond to an additional \$116 billion in GDP or \$4,300 per capita (ABS 2025b, table 1). That said, there is a great deal of uncertainty.

$$\Delta \text{labour productivity} = \Delta \text{GDP} = \frac{\Delta \text{MFP}}{1 - \text{capital income share}} = \frac{\Delta \text{MFP}}{0.53} \quad (7)$$

While AI is likely to significantly boost productivity, some improvements may not be measured. AI is likely to lead to completely new products and improve the quality of existing products. But the contribution of new products and quality improvements are likely to be underestimated in official statistics (Feldstein 2017), especially when they are free. This was the case for previous product and service innovations coming out of the information communication technology revolution. For instance, properly accounting for free digital content may have raised measured US GDP growth by 0.11 percentage points between 2005–2015 (Nakamura et al. 2017). Additionally, investments surrounding AI adoption may be challenging to measure, resulting in delayed gains in measured productivity improvement (Brynjolfsson et al. 2021).

It is also hard to predict how micro-level gains will affect macro-level outcomes. Competition issues (Aghion and Bunel 2024, pp. 13–14), worker reallocation to less productive sectors (Filippucci et al. 2025, pp. 22–23) and uptake delays may reduce gains. Conversely, micro-level estimates may not account for benefits from input-output multipliers or the emergence of new types of economic activity (Filippucci et al. 2024, pp. 17, 26). These effects create additional uncertainty about how AI will affect the economy in the medium term.

In the long term, AI has more potential to transform the economy

There are reasons to think that larger gains are possible as the technology behind AI advances. AI capability has been increasing rapidly and AI may revolutionise knowledge work in the future (Altman 2025).

Additionally, AI may accelerate scientific progress (Aghion and Bunel 2024, pp. 1, 12). In the long run, innovation is a key determinant of economic growth for high-income countries (PC 2023a volume 2, pp. 65–66). And a significant amount of private sector innovation is enabled by (predominately public sector) scientific discoveries. For example, the invention of the transistor, computer and world wide web have enabled the digital economy and a standard of living which would have been impossible a century ago. So, if AI does accelerate the pace of scientific discovery, this is likely to lead to a downstream acceleration in product and process innovation leading to faster productivity growth.

Abbreviations

AASB	Australian Accounting Standards Board
ACCC	Australian Competition and Consumer Commission
AGI	Artificial general intelligence
AI	Artificial intelligence
API	Application Programming Interface
APPs	Australian Privacy Principles
ASIC	Australian Securities and Investments Commission
ATO	Australian Taxation Office
BLADE	Business Longitudinal Analysis Data Environment
CCA	Competition and Consumer Act 2010 (Cth)
CDR	Consumer Data Right
CSV	Comma separated values
DISR	The Department of Industry, Science and Resources
EDGAR	Electronic Data Gathering, Analysis and Retrieval
EU	European Union
EUR	Euro
GDP	Gross domestic product
GDPR	General Data Protection Regulation
HTML	HyperText Markup Language
IFRS	International Financial Reporting Standards
IP address	Internet Protocol address
iXBRL	Inline eXtensible Business Reporting Language
LLM	Large language model
MFP	Multifactor productivity
MHR	My Health Record
OAIC	Office of the Australian Information Commissioner
OECD	Organisation for Economic Co-operation and Development
PC	Productivity Commission
PDF	Portable Document Format
PIMS	Personal Information Management Systems
PoS	Point of Sale

qr	Questionnaire response
SBR	Standard Business Reporting
TDM	Text and data mining
TGA	Therapeutic Goods Administration
UK	United Kingdom
US	United States
USD	United States dollar
US SEC	United States Securities and Exchange Commission
WEF	World Economic Forum
XBRL	eXtensible Business Reporting Language

References

- AASB (Australian Accounting Standards Board) 2019, *Submission to Parliamentary Joint Committee on Corporations and Financial Services inquiry into regulation of auditing in Australia*.
- 2024a, *Climate-related disclosures*, AASB S2.
- 2024b, *General requirements for disclosure of sustainability-related financial information [voluntary]*, AASB S1.
- ABA, ACCI, ACS, ADMA, AFIA, BCA, BSA, DIGI, IAB and ICA (Australian Banking Association, Australian Chamber of Commerce and Industry, Australian Computer Society, Association for Data-driven Marketing and Advertising, Australian Finance Industry Association, Business Council of Australia, Business Software Alliance, Communications Alliance Ltd, Digital Industry Group Inc, Interactive Advertising Bureau, Insurance Council of Australia and Tech Council of Australia) 2024, *Enhancing the Privacy Act 1988 (Cth) Review – Joint Industry Associations Concerns and Recommendations*, www.ag.gov.au/rights-and-protections/freedom-information/freedom-information-disclosure-log/foi24404 (accessed 24 June 2025).
- 2020a, *Inquiry into future directions for the Consumer Data Right*.
- 2020b, *Submission to Attorney-General's Department Privacy Act review – issues paper*.
- 2023, *Screen scraping consultation submission to Treasury*.
- ABC (Australian Broadcasting Corporation) 2020, *Submission to Attorney-General's Department Privacy Act review – issues paper*.
- ABS (Australian Bureau of Statistics) 2024a, *Benefits of and barriers to innovation*, Innovation in Australian businesses, www.abs.gov.au/statistics/industry/technology-and-innovation/innovation-australian-business/2022-23 (accessed 14 July 2025).
- 2024b, *BLADE*, Business activity statements and Australian business register, ABS Datalab. Findings based on use of BLADE data.
- 2024c, *Counts of Australian businesses, including entries and exits*, www.abs.gov.au/statistics/economy/business-indicators/counts-australian-businesses-including-entries-and-exits/jul2020-jun2024 (accessed 11 July 2025).
- 2024d, *Retail trade*, www.abs.gov.au/statistics/industry/retail-and-wholesale-trade/retail-trade-australia/may-2025 (accessed 11 July 2025).
- 2025a, *Australian industry*, www.abs.gov.au/statistics/industry/industry-overview/australian-industry/2023-24 (accessed 18 July 2025).
- 2025b, *Australian system of national accounts*, www.abs.gov.au/statistics/economy/national-accounts/australian-system-national-accounts/2023-24 (accessed 11 July 2025).
- 2025c, *Consumer price index, Australia*, www.abs.gov.au/statistics/economy/price-indexes-and-inflation/consumer-price-index-australia/mar-quarter-2025 (accessed 11 July 2025).
- 2025d, *Estimates of industry multifactor productivity*, www.abs.gov.au/statistics/industry/industry-overview/estimates-industry-multifactor-productivity/2023-24 (accessed 11 July 2025).
- 2025e, *Labour Account*, www.abs.gov.au/statistics/labour/labour-accounts/labour-account-australia/mar-2025 (accessed 25 November 2025).
- ACC (Australian Copyright Council) 2024a, *An introduction to copyright in Australia*, Sydney.
- 2024b, *Fair dealing: what can I use?*, Sydney.
- ACCC (Australian Competition and Consumer Commission) 2021, *Agricultural machinery market study*.
- 2023, *Screen scraping – policy and regulatory implications discussion paper*.
- 2024a, *Designated complaints*, www.accc.gov.au/about-us/designated-complaints (accessed 3 July 2025).
- 2024b, *Digital platform services inquiry*, Interim report 8.
- 2024c, *Framing the future of financial services: strengthening competition and consumer engagement*, www.accc.gov.au/about-us/news/speeches/framing-the-future-of-financial-services-strengthening-competition-and-consumer-engagement (accessed 22 July 2025).
- 2025a, *About the motor vehicle information scheme*.
- 2025b, *The Consumer Data Right*.
- Accenture 2024a, *Consumer Data Right strategic review*.
- 2024b, *Submission to the Department of Industry, Science and Resources Introducing mandatory guardrails for AI in high-risk settings: proposals paper*.
- Accounting Standards Committee of Germany 2025, *Submission to European Securities and Markets Authority's consultation on the ESEF RTS for sustainability reporting and on the amendments to the EEAP RTS – consultation paper*.
- Acemoglu, D 2025, 'The simple macroeconomics of AI', Oxford University Press, *Economic Policy*, vol. 40, no. 121, pp. 13–58.
- ACTU (Australian Council of Trade Unions) 2024, *No future without workers: submission by the Australian Council of Trade Unions to the Select Committee on Artificial Intelligence (AI)*.
- ADHA (Australian Digital Health Agency) 2025, *Expanded investment in Allied Health to accelerate connected care*.
- Adobe 2020, *Submission to Attorney-General's Department Privacy Act review – issues paper*.
- AFIA (Australian Finance Industry Association) 2023, *Screen scraping: policy and regulatory implications*.
- AFMA (Australian Financial Markets Association) 2020, *Submission to Attorney-General's Department Privacy Act review – issues paper*.
- AGD (Attorney-General's Department) 2022a, *Copyright basics*, www.ag.gov.au/rights-and-protections/copyright/copyright-basics (accessed 27 May 2025).
- 2022b, *Copyright enforcement review*, consultations.ag.gov.au/rights-and-protections/copyright-enforcement-review/ (accessed 4 July 2025).

- 2023a, *Copyright and Artificial Intelligence Reference Group (CAIRG)*, www.ag.gov.au/rights-and-protections/copyright/copyright-and-artificial-intelligence-reference-group-cairg (accessed 27 May 2025).
- 2023b, *Copyright enforcement review 2022-23*, www.ag.gov.au/rights-and-protections/copyright/copyright-enforcement-review-2022-23 (accessed 4 July 2025).
- 2023c, *Issue summary paper: artificial intelligence (AI) and copyright*.
- 2023d, *Privacy Act review report*.
- 2024, *Copyright material as AI inputs*, Canberra.
- Aghion, P and Bunel, S 2024, *AI and growth: where do we stand*, Working paper, Federal Reserve Bank of San Francisco.
- , Jones, B and Jones, C 2017, *Artificial intelligence and economic growth*, National Bureau of Economic Research.
- AGL Energy 2020, *Submission to Attorney-General's Department Privacy Act review – issues paper*.
- AI CPA and XBRL International (Association of International Certified Professional Accountants and XBRL International) 2018, *XBRL costs for small reporting companies have declined 45% since 2014*.
- Ai Group 2020, *Submission to Attorney-General's Department Privacy Act review – issues paper*.
- AICD (Australian Institute of Company Directors) 2025, *Corporations Act 2001*, www.aicd.com.au/regulatory-compliance/corporation-act.html (accessed 4 June 2025).
- Allens 2020, *The forgotten shield: how copyright can protect the value of your data*.
- Allison, C 2025, *Best Strava compatible sports watches and smartwatches*.
- ALRC (Australian Law Reform Commission) 1983, *Privacy*.
- 2007, *Review of Australian Privacy Law*.
- 2013, *Copyright and the digital economy*, IP 42, Queensland.
- Altman, S 2025, *Three observations*, blog.samaltman.com/three-observations (accessed 3 July 2025).
- Amazon 2025, *Introducing Vulcan: Amazon's first robot with a sense of touch*.
- Apple Developer nd, *HealthKit*.
- ARCA (Australian Retail Credit Association) 2020, *Submission to Attorney-General's Department Privacy Act review – issues paper*.
- ART (Australian Retirement Trust) 2025, *Understanding your Annual Statement*, www.australianretirementtrust.com.au/newsroom/understanding-your-annual-statement (accessed 21 July 2025).
- ASIC (Australian Securities and Investments Commission) 2018, *Lodgement of financial reports*, asic.gov.au/regulatory-resources/financial-reporting-and-audit/preparers-of-financial-reports/lodgement-of-financial-reports/ (accessed 10 June 2025).
- 2020, *RG 273 Mortgage brokers: best interests duty*, asic.gov.au/regulatory-resources/find-a-document/regulatory-guides/rg-273-mortgage-brokers-best-interests-duty/ (accessed 23 May 2025).
- 2021, *ASIC's digital financial reporting webinar [video]*, YouTube, www.youtube.com/watch?v=VtcsAI53xAs (accessed 30 April 2024).
- 2022, *ePayments code*.
- 2025a, *Digital financial reports*, asic.gov.au/regulatory-resources/financial-reporting-and-audit/preparers-of-financial-reports/digital-financial-reports/ (accessed 27 February 2025).
- 2025b, *Search fees*, www.asic.gov.au/online-services/search-asic-registers/search-fees/ (accessed 10 July 2025).
- ATO (Australian Taxation Office) 2021, *What STP is*, www.ato.gov.au/businesses-and-organisations/hiring-and-paying-your-workers/single-touch-payroll/what-is-stp (accessed 3 March 2025).
- 2023, *ATO digital strategy 2022-25*.
- 2024, *eInvoicing – a better way to do business*.
- AusAgritech 2025, *2024 Australian AusAgritech Sector Report*.
- Australian Government 2017, *Australian Government response to the Productivity Commission inquiry into intellectual property arrangements*, Canberra.
- 2019, *Budget Paper No. 2*, Budget Measures 2019-20.
- 2022, *Consumer Data Right (Telecommunications Sector) Designation 2022*.
- Autor, D 2024, *Applying AI to rebuild middle class jobs*, NBER Working paper series, National Bureau of Economic Research.
- , Levy, F and Murnane, R 2003, 'The skill content of recent technological change: an empirical exploration', *The Quarterly Journal of Economics*, vol. 118, no. 4, pp. 1279–1333.
- Babina, T, Bahaj, S, Buchak, G, De Marco, F, Foulis, A, Gornall, W, Mazzola, F and Yu, T 2025, 'Customer data access and fintech entry: early evidence from open banking', *Journal of Financial Economics*, vol. 169.
- Baily, MN, Brynjolfsson, E and Korinek, A 2023, *Machines of mind: the case for an AI-powered productivity boom*, Brookings Institution.
- Bengio, Y 2025, *International AI safety report*, United Kingdom.
- Bergeaud, A 2024, 'The past, present and future of European productivity', presented at the *ECB Forum on Central Banking*.
- Bhattacharya, N, Cho, YJ and Kim, JB 2018, 'Leveling the playing field between large and small institutions: evidence from the SEC's XBRL mandate', *The Accounting Review*, vol. 93, no. 5, pp. 51–71.
- Bick, A, Blandin, A and Deming, DJ 2024, *The rapid adoption of generative AI*, National Bureau of Economic Research.
- Bill Hero 2024, *Bill Hero – how it works*, www.billhero.com.au/how-it-works.
- Black, J 2007, *Principles based regulation: risks, challenges and opportunities*.
- Blankespoor, E, Miller, B and White, H 2014, 'Initial evidence on the market impact of the XBRL mandate', *Review of Accounting Studies*, vol. 19, pp. 1468–1503.
- Blind, K, Niebel, C and Rammer, C 2023, 'The impact of the EU General data protection regulation on product innovation', *Industry and Innovation*, vol. 31, no. 3, pp. 311–351.
- Briggs, J and Kodnani, D 2023, *The potentially large effects of artificial intelligence on economic growth*, Goldman Sachs.
- Brynjolfsson, E, Li, D and Raymond, L 2025, 'Generative AI at work', Oxford University Press / USA, *Quarterly Journal of Economics*, vol. 140, no. 2, pp. 889–942.
- , Rock, D and Syverson, C 2021, 'The productivity J-curve: how intangibles complement general purpose technologies', *American Economic Journal: Macroeconomics*, vol. 13, no. 1, pp. 333–372.

CA ANZ (Chartered Accountants Australia and New Zealand) 2024, *Australian retail investor confidence 2024*.

— 2025, *Digital reporting now: empowering companies, investors, and the economy*.

— and Wells, P 2020, *The future of financial reporting: what size do you want?*

Castro, D and Steinberg, M 2017, *Blocked: why some companies restrict data access to reduce competition and how open APIs can help*, Center for data innovation, www2.datainnovation.org/2017-open-apis.pdf (accessed 21 July 2025).

Catch Power 2025, *CATCH control: the smart standard*, www.catchpower.com.au/catchcontrol-1 (accessed 21 July 2025).

Cazzaniga, M, Jaumotte, F, Li, L, Melina, G, Panton, AJ, Pizzinelli, C, Rockall, E and Tavares, MM 2024, *Gen-AI: artificial intelligence and the future of work*, IMF Staff Discussion Note SDN2024/001, International Monetary Fund, Washington, DC.

CCAF (Cambridge Centre for Alternative Finance) 2024, *The global state of Open Banking and Open Finance*.

CDEI (Centre for Data Ethics and Innovation) 2022, *Unlocking the value of data: exploring the role of data intermediaries*.

CFIT (Centre for Finance, Innovation and Technology) 2024, *Embracing the UK's Open Finance opportunity*.

Charley, S 2024, 'Physics beyond the imaginable', *Symmetry Magazine*, 9 March.

Chen, M 2023, *What is AI model training & why is it important?*, Oracle, www.oracle.com/au/artificial-intelligence/ai-model-training/ (accessed 27 May 2025).

Chen, Y 2010, *Realizing the full potential of XBRL in government: case studies of XBRL implementation*, IBM Center for The Business of Government.

CHOICE 2020, *Submission to Attorney-General's Department Privacy Act review – issues paper*.

— 2021, *Data collection by loyalty programs*, www.choice.com.au/consumers-and-data/data-collection-and-use/who-has-your-data/articles/loyalty-program-data-collection (accessed 23 July 2025).

— 2024, *Drive one of these car brands? This is how much data they're tracking*, www.choice.com.au/consumers-and-data/data-collection-and-use/who-has-your-data/articles/connected-cars-tracking-your-data (accessed 18 July 2025).

Chui, M, Hazan, E, Roberts, R, Singla, A, Smaje, K, Sukharevsky, A, Yee, L and Zimmel, R 2023, *The economic potential of generative AI*, McKinsey & Company.

CIPL (Centre for Information Policy Leadership) 2024, *The GDPR's first six years positive impacts, remaining implementation challenges, and recommendations for improvement*.

Coles 2025, *Digital receipts*, www.coles.com.au/help/switch-digital-receipts (accessed 16 July 2025).

Commonwealth Bank of Australia 2024a, *Customer safety, convenience and recognition boosted by early implementation of Gen AI*.

— 2024b, *Submission to the Department of Industry, Science and Resources Introducing mandatory guardrails for AI in high-risk settings: proposals paper*.

Communications Alliance Ltd 2020, *Submission to Attorney-General's Department Privacy Act review – issues paper*.

Cowan, P 2016, 'Tax office claims \$1 billion in savings from SBR', *iNews*, 3 August, www.itnews.com.au/news/tax-office-claims-1-billion-in-savings-from-sbr-432460 (accessed 3 March 2025).

CPRC (Consumer Policy Research Centre) 2020, *CPRC 2020 data and technology consumer survey*.

CSIRO (Commonwealth Scientific and Industrial Research Organisation) 2023, *Australia's AI ecosystem momentum*, Canberra.

Dale, L and Heath, NM 2023, *Farm Data Code Update: Responsible Data Practices in Agriculture*, HWL Ebsworth Lawyers.

DBT (Department for Business & Trade) 2024, *The Smart Data Roadmap: action the government is taking in 2024 to 2025*, Government of United Kingdom, UK.

Debreceeny, R, Farewell, S, Piechocki, M, Felden, C and Graning, A 2010, 'Does it add up? Early evidence on the data quality of XBRL filings to the SEC', *Journal of Accounting and Public Policy*, vol. 29, pp. 296–306.

—, — and Verkruijsse, H 2012, *The implications of XBRL for financial statement audit*.

Deepmind 2020, *AlphaFold: a solution to a 50-year-old grand challenge in biology*.

Deloitte 2023, *The ecosystem imperative digital transformation of financial services and moving from Open Banking to Open Data*.

— 2024a, *Consumer data revolution: empowering Australia's future*.

— 2024b, *Generative AI in Asia Pacific: Young employees lead as employers play catch-up*, www2.deloitte.com/us/en/insights/topics/emerging-technologies/generative-ai-adoption-asia-pacific-region.html (accessed 10 July 2025).

Deloitte Access Economics 2023, *Embracing the power of digital corporate reporting: a mandate for change*.

Demirer, M, Hernández, DJJ, Li, D and Peng, S 2024, *Data, privacy laws and firm production: evidence from the GDPR*, w32146, NBER working paper series, National Bureau of Economic Research.

Department of Home Affairs 2025, *Voluntary data classification framework*, www.homeaffairs.gov.au/nat-security/files/voluntary-data-classification-framework-fact-sheet.pdf (accessed 21 July 2025).

Devlin, H 2025, 'AI to revolutionise fundamental physics and "could show how universe will end"', *The Guardian*, 3 February.

DHAC (Department of Health and Aged Care) 2024, *Safe and responsible artificial intelligence in health care – legislation and regulation review*.

— 2025, *Frequently Asked Questions Modernising My Health Record (Sharing by Default) Act 2025*.

DHDA (Department of Health, Disability and Ageing) 2025a, *Modernising My Health Record – improved sharing of pathology and diagnostic imaging information*.

— 2025b, *Safe and Responsible Artificial Intelligence in Health Care – Legislation and Regulation Review – Final Report*.

DHL 2024, *How AI enhances last mile delivery for e-commerce success*, www.dhl.com/discover/en-au/ship-with-dhl/start-shipping/benefits-of-artificial-intelligence-in-last-mile-delivery (accessed 1 June 2025).

Digital Health 2019, *Checking in with the Pharmacist Shared Medicines List*.

Digital NSW 2025, *A common understanding: simplified AI definitions from leading standards*, www.digital.nsw.gov.au/

- policy/artificial-intelligence/a-common-understanding-simplified-ai-definitions-from-leading (accessed 2 June 2025).
- DISR (Australian Government Department of Industry, Science and Resources) 2024a, *Proposals paper for introducing mandatory guardrails for AI in high-risk settings*, Safe and responsible AI in Australia.
- 2024b, *Voluntary AI safety standard*, National Artificial Intelligence Centre.
- DLA Piper 2025, *The European Commission considers pause on AI Act's entry into application*, www.dlapiper.com/en-gb/insights/publications/ai-outlook/2025/the-european-commission-considers-pause-on-ai-act-entry-into-application (accessed 30 June 2025).
- DSIT (Department for Science, Innovation & Technology) 2024, *UK business data survey 2024*, UK Government.
- DTB (Department for Business & Trade) 2025, *Smart Data Discovery Challenge – significant insights and outcomes*.
- DTI (Data transfer initiative) 2018, *Data Transfer Project overview and fundamentals*.
- 2024a, *A third-party trust model for direct personal data transfers*.
- 2024b, *The present and future of data portability*.
- Du, H, Vasarhelyi, MA and Zheng, X 2013, 'XBRL mandate: thousands of filing errors and so what?', *Journal of Information Systems*, vol. 27, no. 1, pp. 61–78.
- Duball, J 2025, '"We cannot be left behind:" How Canada is balancing AI regulation, innovation', *IAPP*, 21 May.
- EC (European Commission) 2024, *The Digital Markets Act: ensuring fair and open digital markets*, commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en (accessed 22 July 2025).
- 2025a, *Data Act*, digital-strategy.ec.europa.eu/en/policies/data-act (accessed 22 July 2025).
- 2025b, *Proposal postponing the application of some reporting requirements in the CSRD and the transposition deadline and application of the CSDDD*, Omnibus I-COM(2025)80.
- EESS (Electrical Equipment Safety System) 2025, *Essential safety criteria*, www.eess.gov.au/safety-requirements/essential-safety-criteria/ (accessed 23 May 2025).
- EIG (Economist Impact Group) 2023, *Open access: the future of data portability*.
- Elliott, RA, Many Angley, Deirdre T Criddle, Fatemeh Emadi, Shania Liu, and Jonathan Penm 2024, 'Achieving safe medication management during transitions of care from hospital: time for a stewardship approach', *Australian Prescriber*, vol. 47, pp. 106–108.
- Ellis, V 2025, 'Rangers use drones to survey north Australia coastline for ghost nets', *ABC News*, 9 February, www.abc.net.au/news/2025-02-09/ghost-nets-found-along-north-australia-coast-with-help-of-drones/104867912 (accessed 1 June 2025).
- Eloundou, T, Manning, S, Mishkin, P and Rock, D 2024, 'GPTs are GPTs: labor market impact potential of LLMs', American Association for the Advancement of Science, *Science*, vol. 384, no. 6702, pp. 1306–1308.
- Elvery, S and Tan, T 2025, 'Parents asked to read "Moby Dick" terms, as criminals target kids' data', *ABC News*, 26 February, www.abc.net.au/news/2025-02-27/classroom-apps-technology-kids-data-terms-conditions/104966952 (accessed 15 May 2025).
- EnergyFlex 2025, *EnergyFlex*.
- ESMA (European Securities and Markets Authority) 2016, *Feedback statement on the consultation paper on the Regulatory Technical Standard on the European Single Electronic Format*.
- European Parliament 2023a, *EU AI Act: first regulation on artificial intelligence*, www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence (accessed 1 June 2025).
- 2023b, *Regulation (EU) 2023/2854 of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)*.
- 2023c, *Shaping the digital transformation: EU strategy explained*.
- Evans, B, Lim, C, Hawthorne, L, Pallaras, L and Hall, E 2024, *Risks of Gen AI – safeguarding intellectual property in the AI era*, www.kwm.com/au/en/insights/latest-thinking/risks-of-gen-ai-safeguarding-intellectual-property-in-the-ai-era.html (accessed 29 May 2025).
- Everyday Rewards 2025, *Top frequently asked questions*, www.everyday.com.au/rewards/app.html (accessed 16 July 2025).
- Expand 2025, *Annual statements and reports available soon*, www.myexpand.com.au/annual-statements-and-reports (accessed 21 July 2025).
- Export Finance Australia 2023, *Australia—AI adoption creates benefits and challenges for businesses*, www.exportfinance.gov.au/resources/world-risk-developments/2023/may/australia-ai-adoption-creates-benefits-and-challenges-for-businesses/ (accessed 4 June 2025).
- Exposito-Rosso, S, Cao, F-X, Piquet, A and Medjaoui, M 2022, *GDPR data portability: the forgotten right*.
- Eyers, J 2020, 'CBA says using fintechs exposes customers to account fraud', *Australian Financial Review*, 16 March.
- Facebook 2025, *Information available to download from your Facebook profile | Facebook Help Centre*, www.facebook.com/help/384437594328726?helpref=faq_content (accessed 21 July 2025).
- FDATA 2023, *Screen scraping: policy and regulatory implications*.
- Feldstein, M 2017, 'Underestimating the real growth of GDP, personal income, and productivity', *Journal of Economic Perspectives*, vol. 31, no. 2, pp. 145–164.
- Fernandez, RC, Subramaniam, P and Franklin, MJ 2020, *Data market platforms: trading data assets to solve data problems*, arxiv.org/abs/2002.01047 (accessed 22 July 2025).
- Field, S 2025, 'No more smashed avo: the Aussie robot fixing farming's delicate problem', *Forbes Australia*, 3 March.
- Filippucci, F, Gal, P, Laengle, K and Schief, M 2025, *Macroeconomic productivity gains from artificial intelligence in G7 economies*, 41, OECD Artificial Intelligence Papers, OECD.
- , — and Schief, M 2024, *Miracle or myth? Assessing the macroeconomic productivity gains from artificial intelligence*, OECD Publishing.
- Fintech Australia 2023, *Screen scraping: policy and regulatory implications*.
- FormX 2025, *PDF scraping: how to extract unstructured data from PDFs?*, www.formx.ai/blog/pdf-scraping-extract-unstructured-data-from-pdfs (accessed 21 July 2025).

- Foshag, TA 2025, *The capital market effects of machine-readable data errors: evidence from XBRL US Data Quality Committee rules*.
- Fraser, D and Anderson Dykema, S 2025, *The demise of the Artificial Intelligence and Data Act (AIDA): 5 key lessons*, McInnes Cooper.
- Frollo 2024, *Consumer Data Right draft rules: consent review and operational enhancements*.
- Gao, L, Chen, Z, Zhao, W and Lai, X 2025, 'Does cybersecurity regulation reduce corporate data-breach risk?', *Finance Research Letters*, vol. 78, p. 107171.
- Goldberg, SG, Johnson, GA and Shriver, SK 2024, 'Regulating privacy online: An economic evaluation of the GDPR', *American Economic Journal: Economic Policy*, vol. 16, no. 1, pp. 325–358.
- Goldstein, P, Stuetzle, C and Bischoff, S 2024a, *Kneschke vs. LAION – landmark ruling on TDM exceptions for AI training data – part 1*, *Kluwer Copyright Blog*, copyrightblog.kluweriplaw.com/2024/11/13/kneschke-vs-laion-landmark-ruling-on-tdm-exceptions-for-ai-training-data-part-1/ (accessed 17 June 2025).
- , —— and —— 2024b, *Kneschke vs. LAION – landmark ruling on TDM exceptions for AI training data – part 2*, *Kluwer Copyright Blog*, copyrightblog.kluweriplaw.com/2024/11/14/kneschke-vs-laion-landmark-ruling-on-tdm-exceptions-for-ai-training-data-part-2/ (accessed 17 June 2025).
- Google 2020, *Submission to Attorney-General's Department Privacy Act review – issues paper*.
- Government of Canada 2025, *The Artificial Intelligence and Data Act (AIDA) – companion document*.
- Gulati-Gilbert, S and Seamans, R 2023, 'Data portability and interoperability: a primer on two policy tools for regulation of digitized industries', *Brookings*.
- Gupta, C 2023a, *In whose interest: why businesses need to keep consumers safe and treat their data with care*.
- 2023b, *Not a fair trade: consumer views on how businesses use their data*.
- Harris, TS and Morsfield, S 2012, *An evaluation of the current state and future of XBRL and interactive data for investors and analysts*, White paper, 3, Columbia Business School Center for Excellence in Accounting and Security Analysis.
- Harrison, K 2023, *Australia's privacy laws demand reform to better protect consumers*, www.unsw.edu.au/law-justice/our-research/impact/australia-privacy-laws-demand-reform-better-protect-consumers (accessed 9 July 2024).
- Hayne, KM 2019, *Royal Commission into misconduct in the banking, superannuation and financial services industry*, Canberra.
- Helios Salinger 2022, *Privacy Act reforms*, www.salingerprivacy.com.au/privacy-reforms/ (accessed 12 March 2025).
- 2025, *Privacy pulse 2025: measuring maturity*.
- Hoitash, R, Hoitash, U and Morris, L 2020, *eXtensible business reporting language (XBRL): a review and implications for future research*.
- Hollander, S and Litjens, R 2022, *Localised information acquisition*, SSRN 3691111, Tilburg School of Economics and Management.
- IAPP and EY (International Association of Privacy Professionals and Ernst & Young) 2017, *IAPP-EY annual privacy governance report 2017*.
- and —— 2018, *IAPP-EY annual privacy governance report 2018*.
- and —— 2019, *IAPP-EY annual privacy governance report 2019*.
- and —— 2022, *IAPP-EY annual privacy governance report 2022*.
- IBM Australia 2024, *Submission to the Department of Industry, Science and Resources Introducing mandatory guardrails for AI in high-risk settings: proposals paper*.
- IFRS Advisory Council 2022, *Progressing our digital financial reporting strategy: background information on digital financial reporting*, Agenda paper 7B.
- IFRS Foundation 2024, *Digital financial reporting: facilitating digital comparability and analysis of financial reports*.
- IGEA (Interactive Games and Entertainment Association) 2020, *Submission to Attorney-General's Department Privacy Act review – issues paper*.
- Indeed 2024, *Submission to the Department of Industry, Science and Resources Introducing mandatory guardrails for AI in high-risk settings: proposals paper*.
- Inrupt 2022, *Digital Flanders reconnects citizens with their data through Inrupt's solid server*, www.inrupt.com/blog/digital-flanders-reconnects-citizens-with-their-data (accessed 15 July 2025).
- Insurance Council of Australia 2020, *Submission to Attorney-General's Department Privacy Act review – issues paper*.
- Isaacson, R 2024, 'I was a beta tester for the Nobel prize-winning AlphaFold AI – it's going to revolutionise health research', *The Conversation*, 12 October.
- ITI (Information Technology Industry Council) 2020, *Submission to Attorney-General's Department Privacy Act review – issues paper*.
- Janssen, R, Kesler, R, Kummer, ME and Waldfogel, J 2022, *GDPR and the lost generation of innovative apps*.
- Jerez, L 2021, *NAB launches in-app 'smart receipts' for customers*, news.nab.com.au/news/nab-launches-in-app-smart-receipts-for-customers/ (accessed 16 July 2025).
- Jia, J, Jin, GZ and Wagman, L 2021, 'The persisting effects of the EU General Data Protection Regulation on technology venture investment', *Antitrust Source*, vol. 20, no. 6.
- Jones, CI and Tonetti, C 2020, 'Nonrivalry and the economics of data', *American Economic Association 2014 Broadway*, Suite 305, Nashville, TN 37203, *American Economic Review*, vol. 110, no. 9, pp. 2819–2858.
- Jones, S 2024a, *Albanese Government to reset Consumer Data Right*, *Media release*, 8 September.
- 2024b, *Assistant Treasurer Stephen Jones' speech to CEDA*, www.ceda.com.au/newsandresources/news/technology-innovation/assistant-treasurer-stephen-jones-speech-to-ceda (accessed 23 June 2025).
- 2025, *Consumer Data Right expansion to deliver a better deal for consumers*.
- Kemp, K 2020, *Concealed data practices and competition law: why privacy matters*.
- Khan, R 2024, *AI training data dilemma: legal experts argue for 'fair use'*, www.forbes.com/sites/roomykhana/2024/10/04/ai-training-data-dilemma-legal-experts-argue-for-fair-use/ (accessed 17 June 2025).

- Klosek, K and Blumenthal, MS 2024, *Training generative AI models on copyrighted works is fair use*, www.arl.org/blog/training-generative-ai-models-on-copyrighted-works-is-fair-use/ (accessed 17 June 2025).
- Knights, S 2023, *Customised dashboards combine agtech tools*, GroundCover.
- Koski, H and Valmari, N 2020, *Short-term impacts of the GDPR on firm performance*, ETLA Working Papers.
- Kourinian, A 2024, *California passes new generative artificial intelligence law requiring disclosure of training data*, Mayer Brown, www.mayerbrown.com/en/insights/publications/2024/09/california-passes-new-generative-artificial-intelligence-law-requiring-disclosure-of-training-data (accessed 1 June 2025).
- Kowal, E 2025, 'AI is in every NSW public school classroom. Is that a good thing?', *The Age*, 21 June.
- Krämer, J, Senellart, P and de Streel, A 2020, *Making data portability more effective for the digital economy*.
- Last.fm 2025, *Track my music*.
- Lateral Economics 2014, *Open for business: how open data can help achieve the G20 growth target*, Omidyar Network.
- 2019, *Valuing the Australian Census*.
- Lenovo 2024, *What are floating-point operations per second (FLOPS)?*, www.lenovo.com/au/en/glossary/flops/ (accessed 1 June 2025).
- Leprince-Ringuet, D and Partington, M 2025, 'EU could pause AI Act rollout amid industry backlash: "It's really toxic"', *Sifted*, 29 May, sifted.eu/articles/eu-ai-act-pause-analysis (accessed 1 June 2025).
- Leung, V 2022, *What's the difference between Open Banking & Web scraping?*, Open Banking API Platform – Basiq, www.basq.io/blog/comparing-open-banking-and-web-scraping/ (accessed 21 July 2025).
- Levy, M 2022, *Quality of advice review*, ACT.
- Li, OZ, Ni, C and Lin, Y 2012, 'Does XBRL adoption reduce the cost of equity capital?', *Available at SSRN 2131001*.
- LinkedIn 2024, *Submission to the Department of Industry, Science and Resources Introducing mandatory guardrails for AI in high-risk settings: proposals paper*.
- Liu, C and Babar, MA 2024, 'Corporate cybersecurity risk and data breaches: a systematic review of empirical research', *Australian Journal of Management*, vol. 0, no. 0, journals.sagepub.com/doi/full/10.1177/03128962241293658 (accessed 14 July 2025).
- Liu, Y and Wang, H 2024, *Who on earth is using generative AI?*, Policy Research working paper, World Bank Group.
- Liu, Z and Zhang, N 2024, 'The productivity effect of digital financial reporting', Springer, *Review of Accounting Studies*, vol. 29, no. 3, pp. 2350–2390.
- Lohr, AA 2025, *Google/Ipsos multi-country AI survey 2024 – Topline*, www.ipsos.com/en-us/google-ipsos-multi-country-ai-survey-2025 (accessed 1 June 2025).
- Mastercard 2024, *Submission to the Department of Industry, Science and Resources Introducing mandatory guardrails for AI in high-risk settings: proposals paper*.
- McCarthy Hockey, T 2024, 'Remarks to AFIA Risk Summit 2024', presented at AFIA Risk Summit, Melbourne, 22 May.
- McGrath, G, Todd, R, Doneley, C and Hilton, A 2024, *Australia's first tranche of privacy reforms – a deep dive and why they matter*, Ashurst, www.ashurst.com/en/insights/australias-first-tranche-of-privacy-reforms-a-deep-dive-and-why-they-matter/ (accessed 12 March 2025).
- McKinsey Global Institute 2024, *A new future of work: the race to deploy AI and raise skills in Europe and beyond*.
- McLachlan, A 2024, *Second reading speech of the Privacy and Other Legislation Amendment Bill 2024*.
- Microsoft 2020, *Submission to Attorney-General's Department Privacy Act review – issues paper*.
- Milmo, D 2023, 'ChatGPT reaches 100 million users two months after launch', *The Guardian*, 3 February.
- Misch, F, Park, B, Pizzinelli, Carlo and Sher, G 2025, *Artificial intelligence and productivity in Europe*, 67, IMF Working Papers 2025, International Monetary Fund.
- MyShopDash 2025, *MyShopDash – Learn more about your shopping habits*, myshopdash.app/ (accessed 21 July 2025).
- Nakamura, LI, Samuels, J and Soloveichik, RH 2017, *Measuring the 'free' digital economy within the GDP and productivity accounts*, BEA Working Papers, Bureau of Economic Analysis.
- Nasdaq 2019, *Response to United States Securities and Exchange Commission request for comment on earnings releases and quarterly reports (release no. 33-10588)*.
- Newman, LH 2022, *A new jailbreak for John Deere Tractors rides the right-to-repair wave*, www.wired.com/story/john-deere-tractor-jailbreak-defcon-2022/ (accessed 14 July 2025).
- NFF (National Farmers' Federation) 2023a, *Farm data code*.
- 2023b, *Farm data code edition 2*.
- Ng-Loy, WL 2024, 'Copyright exceptions for text and data mining: a case of specificity (certainty) and generality (flexibility)', *Kreation Innovation Märkte – Creation Innovation Markets*, pp. 263–276.
- Nicas, J 2019, 'Apple cracks down on apps that fight iPhone addiction', *New York Times*, 27 April.
- Noy, S and Zhang, W 2023, 'Experimental evidence on the productivity effects of generative artificial intelligence', *American Association for the Advancement of Science, Science*, vol. 381, no. 6654, pp. 187–192.
- NSW Government 2024, *Rent records kept by agents and landlords*.
- OAIC (Office of the Australian Information Commissioner) 2023a, *Australian Privacy Principles*, www.oaic.gov.au/privacy/australian-privacy-principles (accessed 9 July 2024).
- 2023b, *Rights and responsibilities*, www.oaic.gov.au/privacy/privacy-legislation/the-privacy-act/rights-and-responsibilities (accessed 9 July 2024).
- 2023c, *Screen scraping – policy and regulatory implications discussion paper*.
- 2023d, *The Privacy Act*, www.oaic.gov.au/privacy/privacy-legislation/the-privacy-act (accessed 24 April 2025).
- OECD (Organisation for Economic Co-operation and Development) 2019, *Enhancing access to and sharing of data: reconciling risks and benefits for data re-use across societies*, Paris.
- 2021a, *Data portability, interoperability and competition*, OECD, www.oecd.org/en/publications/data-portability-interoperability-and-competition_73a083a9-en.html (accessed 15 July 2025).
- 2021b, *Data portability, interoperability and digital platform competition*, Paris.

- 2021c, *Mapping data portability initiatives, opportunities and challenges*, www.oecd.org/en/publications/mapping-data-portability-initiatives-opportunities-and-challenges_a6edfab2-en.html (accessed 18 July 2025).
- 2022a, *Data shaping firms and markets*, www.oecd.org/en/publications/data-shaping-firms-and-markets_7b1a2d70-en.html (accessed 18 July 2025).
- 2022b, *Measuring the value of data and data flows*, 345, Paris.
- 2023a, *Consumer vulnerability in the digital age*, www.oecd-ilibrary.org/science-and-technology/consumer-vulnerability-in-the-digital-age_4d013cc5-en (accessed 25 July 2025).
- 2023b, *Shifting from Open Banking to Open Finance: Results from the 2022 OECD survey on data sharing frameworks*, Paris.
- 2023, *Using AI to support people with disability in the labour market*, OECD Artificial Intelligence Papers, Paris.
- 2024a, *Artificial intelligence and the changing demand for skills in the labour market*, Paris.
- 2024b, *The impact of data portability on user empowerment, innovation, and competition*, Paris.
- O'Mahoney, J, Berry, C, Herbert, V, Subramanian, A, Chan, A, Hull, N and Wong, B 2022, *Demystifying data*, Deloitte Access Economics.
- Open Finance ANZ 2025, *Australian open banking ecosystem map and report 5th Edition – January 2025*, January.
- OpenAI 2025a, *AI in Australia: OpenAI's economic blueprint*.
- 2025b, *ChatGPT pricing*, openai.com/chatgpt/pricing (accessed 4 July 2025).
- Optus 2020, *Submission to Attorney-General's Department Privacy Act review – issues paper*.
- OurProperty 2025, *How to view your tenant ledger*, OurProperty.
- Parliament of Australia 2024, *Privacy and Other Legislation Amendment Bill 2024*.
- PC (Productivity Commission) 2004, *ICT Use and Productivity: A Synthesis from Studies of Australian Firms*, Commission Research Paper, Canberra.
- 2012, *Impacts and Benefits of COAG Reforms: Business Regulation and VET*, Research Report, Canberra.
- 2017, *Data Availability and Use*, Report no. 82, Canberra.
- 2018, *Competition in the Australian Financial System*, Report no. 89, Canberra.
- 2021, *Right to Repair*, Report no. 97, Canberra.
- 2023a, *5-year Productivity Inquiry: Advancing Prosperity*, Inquiry report no. 100, vol. 1, Canberra.
- 2023b, *5-year Productivity Inquiry: Australia's data and digital dividend*, Inquiry report no. 100, vol. 4, Canberra.
- 2023c, *5-year Productivity Inquiry: Keys to growth*, Inquiry Report no. 100, vol. 2, Canberra.
- 2024a, *Leveraging digital technology in healthcare*.
- 2024b, *Leveraging digital technology in healthcare*, Research paper, Canberra.
- 2024c, *Making the most of the AI opportunity: AI raises the stakes for data policy*, Research paper, no. 3, Canberra.
- 2024d, *Making the most of the AI opportunity: AI uptake, productivity, and the role of government*, Research paper, no. 1, Canberra.
- 2024e, *Making the most of the AI opportunity: The challenges of regulating AI*, Research paper, no. 2, Canberra.
- Perdana, A, Robb, A and Rohde, F 2015, 'An integrative review and synthesis of XBRL research in academic journals', *Journal of Information Systems*, vol. 29, no. 1, pp. 115–153.
- Pinsent Masons 2023, *UK text and data mining copyright exception proposals set to be watered down*, www.pinsentmasons.com/out-law/news/uk-text-and-data-mining-copyright-exception-proposals-set-to-be-watered-down (accessed 17 June 2025).
- PJCCFS (Parliamentary Joint Committee on Corporations and Financial Services) 2009, *Inquiry into financial products and services in Australia*.
- PM&C (Prime Minister and Cabinet) 2021, *Australia data strategy*.
- Ponemon Institute 2018, *The race to GDPR: a study of companies in the United States and Europe*.
- Pressley, JP 2023, *What is FLOPS and how does it help with supercomputer performance?*, biztechmagazine.com/article/2023/08/what-flops-and-how-does-it-help-supercomputer-performance-perfcon (accessed 1 June 2025).
- PwC 2024, *Unlocking Australia's growth potential: insights from the 2024 AI Jobs Barometer*, www.pwc.com.au/services/artificial-intelligence/unlocking-australias-growth-potential.html (accessed 1 June 2025).
- Qantas Money 2025, *Where can I find my statements?*, support.qantasmoney.com/manage-your-account/where-can-i-find-my-premier-statements (accessed 16 July 2025).
- Qu, J, Simes, R and O'Mahony, J 2017, 'How do digital technologies drive economic growth?', *Economic Record*, vol. 93, no. S1, pp. 57–69.
- Queensland Treasury 2022, *Guidance Note: alternatives to traditional regulation*.
- RACGP (Royal Australian College of General Practitioners) 2021, *Electronic prescriptions*.
- RBA (Reserve Bank of Australia) 2024, *Focus topic: financial stability implications of artificial intelligence*, Financial Stability Review – September 2024, www.rba.gov.au/publications/fsr/2024/sep/focus-topic-financial-stability-implications-of-artificial-intelligence.html (accessed 1 June 2025).
- 2025, *Exchange rates*, www.rba.gov.au/statistics/frequency/exchange-rates.html (accessed 23 July 2025).
- ReedSmith 2025, *Court shuts down AI fair use argument in Thomson Reuters Enterprise Centre GMBH v. Ross Intelligence Inc.*, www.reedsmith.com/en/perspectives/2025/03/court-ai-fair-use-thomson-reuters-enterprise-gmbh-ross-intelligence (accessed 17 June 2025).
- Richards, S 2023, 'Artificial intelligence helps catalogue Aboriginal rock art in Far North Queensland', *ABC News*, 15 September.
- RMIT University 2024, *Submission to the Department of Industry, Science and Resources Introducing mandatory guardrails for AI in high-risk settings: proposals paper*.
- Rowland, M 2024, *New Duty of Care obligations on platforms will keep Australians safer online*, Department of Infrastructure, Transport, Regional Development, Communications and the Arts, minister.infrastructure.gov.au/rowland/media-release/new-duty-care-obligations-platforms-will-keep-australians-safer-online (accessed 17 March 2025).

- Ryan, J 2023, 'ChatGPT and other AI models were trained on copyrighted books. Can they be "untrained"?', *ABC News*, 29 November.
- Safe Work Australia 2011, *How to manage work health and safety risks*.
- 2025, *Codes of practice*, www.safeworkaustralia.gov.au/law-and-regulation/codes-practice (accessed 23 May 2025).
- Salvator, D 2025, *Explaining tokens — the language and currency of AI*, blogs.nvidia.com/blog/ai-tokens-explained/ (accessed 2 June 2025).
- Schwarcz, D, Manning, S, Barry, P, Cleveland, DR, Prescott, J and Rich, B 2025, 'AI-powered lawyering: AI reasoning models, retrieval augmented generation, and the future of legal practice'.
- ScienceDaily 2024, *Autonomous synthesis robot uses AI to speed up chemical discovery*, www.sciencedaily.com/releases/2024/01/240125145938.htm (accessed 2 June 2025).
- Scott, L 2024, *How to use Strava with your smartwatch*, TechRadar, www.techradar.com/health-fitness/fitness-apps/how-to-use-strava-with-your-smartwatch (accessed 21 July 2025).
- SEEK Limited 2024, *Submission to the Department of Industry, Science and Resources Introducing mandatory guardrails for AI in high-risk settings: proposals paper*.
- Senftleben, M 2022, 'Compliance of national TDM rules with international copyright law: an overrated nonissue?', *IIC – International Review of Intellectual Property and Competition Law*, vol. 53, pp. 1477–1505.
- Service, R 2020, 'The game has changed.' *AI triumphs at solving protein structures*, www.science.org/content/article/game-has-changed-ai-triumphs-solving-protein-structures (accessed 2 June 2025).
- Skript 2024, *Consumer Data Right Rules: consent and operational enhancement amendments consultation*.
- Slyp 2025, *Slyp digital receipts*.
- Smedes, M, Nguyen, T and Tenburren, B 2022, *Valuing data as an asset, implications for economic measurement*, Economic implications of the digital economy conference, Australian Bureau of Statistics.
- Snowden, A 2025a, 'Could Minter Ellison using AI to speed up discovery process mean less graduate lawyer jobs?', *The Australian*, 6 May.
- 2025b, 'Pushing generative AI to its limits': How top Australian law firms are leaning into AI', *The Australian*, 12 May.
- South African CIPC (South African Companies and Intellectual Property Commission) 2024, *XBRL programme*, www.cipc.co.za/?page_id=4400 (accessed 6 May 2025).
- Square 2022, *Spotlight on Xero: accounting software that seamlessly integrates with Square*, squareup.com/au/en/the-bottom-line/inside-square/xero-integration-for-square (accessed 14 July 2025).
- Stanford HAI (Stanford University Human-Centred Artificial Intelligence) 2025, *Artificial Intelligence Index report 2025*.
- Stryker, C 2024, *What is multimodal AI?*, www.ibm.com/think/topics/multimodal-ai (accessed 2 June 2025).
- and Kavlakoglu, E 2024, *What is artificial intelligence (AI)?*, www.ibm.com/think/topics/artificial-intelligence (accessed 2 June 2025).
- Svanberg, M, Li, W, Fleming, M, Goehring, B and Thompson, N 2024, 'Beyond AI exposure: which tasks are cost-effective to automate with computer vision?', *Available at SSRN 4700751*.
- Tawiah, V and Borgi, H 2022, 'Impact of XBRL adoption on financial reporting quality: a global evidence', *Accounting Research Journal*, vol. 35, no. 6, pp. 815–833.
- Taylor, A, Friedman, C and Fishel, G 2025, 'State AGs fill the AI regulatory void', *Reuters*, 20 May.
- TCA (Transport Certification Australia) 2025, *RIM industry-led data-sharing schemes (Aus)*.
- Telstra 2024a, *Submission to the Department of Industry, Science and Resources Introducing mandatory guardrails for AI in high-risk settings: proposals paper*.
- 2024b, *Telstra scales up AI adoption following promising pilots of generative AI solutions improving customer experience*, www.telstra.com.au/aboutus/media/media-releases/telstra-scales-up-ai-adoption (accessed 2 June 2025).
- Tenants' Union of NSW 2025, *Rent payment factsheet*, *Tenants rights factsheet*.
- TGA (Therapeutic Goods Administration) 2024, *TGA consultation: Clarifying and strengthening the regulation of Artificial Intelligence (AI)*.
- 2025, *Clarifying and strengthening the regulation of medical device software including artificial intelligence (AI)*.
- The Guardian Australia 2020, *Submission to Attorney-General's Department Privacy Act review – issues paper*.
- The University of Melbourne 2024, *Submission to the Department of Industry, Science and Resources Introducing mandatory guardrails for AI in high-risk settings: proposals paper*.
- The University of Notre Dame Australia 2024, *Copyright: an overview*, library.nd.edu.au/c.php?g=861182&p=7054290 (accessed 27 May 2025).
- The White House 2025a, *Accelerating federal permitting of data center infrastructure*, Executive Orders.
- 2025b, *Preventing woke AI in the federal government*, Executive Orders.
- 2025c, *Promoting the export of the American AI technology stack*, Executive Orders.
- 2025d, *Winning the Race: America's AI Action Plan*.
- Trakt.Tv 2025, *Discover. Track. Share*.
- Treasury (Australian Government Treasury) 2019, *Reducing the financial reporting burden for SMEs*, treasury.gov.au/small-business/frt/factsheet (accessed 27 March 2025).
- 2021, *Consumer data right: Telecommunications sectoral assessment: Final Report*.
- 2022a, *Consumer Data Right – strategic assessment outcomes*, Department of the Treasury.
- 2022b, *Statutory review of the Consumer Data Right report*.
- 2023a, *CDR consent review: CDR rules and data standards design paper*, Canberra.
- 2023b, *Consumer Data Right compliance costs review*.
- 2023c, *Screen scraping – policy and regulatory implications*.
- 2024, *Review of AI and the Australian Consumer Law*.
- 2025a, *Consumer Data Right*, treasury.gov.au/policy-topics/economy/consumer-data-right (accessed 1 July 2025).

—— 2025b, *Review of the Motor Vehicle Service and Repair Information Sharing Scheme*, Discussion paper.

Troshani, I and Rowbottom, N 2021, 'Digital corporate reporting: research developments and implications', *Australian Accounting Review*, vol. 31, no. 98, pp. 213–232.

—— and —— 2022, *Digital corporate reporting: global experiences from the G20 and implications for policy formulation*, CPA Australia.

UK FRC (United Kingdom Financial Reporting Council) 2025, *Structured digital reporting – 2024/25 insights*, www.frc.org.uk/library/digital-reporting/structured-digital-reporting-202425-insights/ (accessed 16 May 2025).

UK Government 2024, *Copyright and AI: consultation*, www.gov.uk/government/consultations/copyright-and-artificial-intelligence/copyright-and-artificial-intelligence (accessed 17 June 2025).

UK Intellectual Property Office 2014, *Guidance: exceptions to copyright*, www.gov.uk/guidance/exceptions-to-copyright (accessed 17 June 2025).

UK Parliament 2025, *Data (Use and Access) Act 2025 (UK)*, No. 18.

US SEC (United States Securities and Exchange Commission) 2024a, *IFRS Taxonomy*, www.sec.gov/data-research/standard-taxonomies/ifrs-taxonomy (accessed 10 July 2025).

—— 2024b, *Semi-annual report to Congress regarding public and internal use of machine-readable data for corporate disclosures*.

—— 2024c, *Smaller reporting companies*, www.sec.gov/resources-small-businesses/going-public/smaller-reporting-companies (accessed 30 June 2025).

—— 2025, *EDGAR XBRL validation errors*, www.sec.gov/data-research/xbrl-validation-rendering/edgar-xbrl-validation-errors (accessed 21 May 2025).

VLRC (Victorian Law Reform Commission) 2002, *Defining Privacy*.

VTHC (Victorian Trades Hall Council) 2025, *Submission to the Select Committee on Adopting Artificial Intelligence*.

Wang, B, Weng, L, Wu, Q and Xu, EX 2024, *Do machine-readable disclosures facilitate regulatory scrutiny? Evidence from SEC comment letters*, SSRN 4989482, Northeastern University D'Amore-McKim School of Business.

Wang, Y, Ren, Y, Qian, L, Peng, X, Wang, K, Han, Y, Feng, D, Liu, X-Y, Huang, J and Xie, Q 2025, *FinTagging: an LLM-ready benchmark for extracting and structuring financial information*, arXiv:2505.20650.

Weatherall, K 2020, *Submission to Attorney-General's Department Privacy Act review – issues paper*.

WEF (World Economic Forum) 2022, *Advancing digital agency: the power of data intermediaries*.

—— 2025, *Future of jobs report 2025*.

WeMoney 2024, *Consultation response – CDR rules: consent and operational enhancement amendments*.

—— 2025, *WeMoney*.

Westpac 2024, *Submission to the Department of Industry, Science and Resources Introducing mandatory guardrails for AI in high-risk settings: proposals paper*.

—— 2025, *Westpac deploys real-time AI to take on scammers*.

White & Case 2025, *AI watch: global regulatory tracker – Japan*, www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-japan (accessed 2 June 2025).

White, JW, Finnegan, OL, Tindall, N, Nelakuditi, S, Brown, DE, Pate, RR, Welk, GJ, de Zambotti, M, Ghosal, R, Wang, Y, Burkart, S, Adams, EL, Chandrashekhar, M, Armstrong, B, Beets, MW and Weaver, RG 2024, 'Comparison of raw accelerometry data from ActiGraph, Apple Watch, Garmin, and Fitbit using a mechanical shaker table', *PLOS ONE*, vol. 19, no. 3, www.ncbi.nlm.nih.gov/pmc/articles/PMC10980217/ (accessed 21 July 2025).

White, O, Madgavkar, A, Townsend, Z, Manyika, J, Olanrewaju, T, Sibanda, T and Kaufman, S 2021, *Financial data unbound: The value of open data for individuals and institutions*, McKinsey Global Institute.

Wolford, B 2019, *What is GDPR, the EU's new data protection law?*, gdpr.eu/what-is-gdpr/ (accessed 4 June 2025).

Woolworths Group 2022, *Submission to Attorney-General's Department Privacy Act review – discussion paper*.

Workiva 2022, *How Challenger Limited accelerated finance transformation*, www.workiva.com/en-au/customers/how-challenger-limited-accelerated-finance-transformation (accessed 26 June 2025).

World Bank 2025, *PPP conversion factor, Australia*, data.worldbank.org/indicator/PA.NUS.PPP?locations=AU (accessed 30 June 2025).

XBRL International 2024, *Australia aligns climate disclosures with international standards after extensive consultation*, www.xbrl.org/news/australia-aligns-climate-disclosures-with-international-standards-after-extensive-consultation/ (accessed 29 April 2025).

XBRL UK Jurisdiction 2013, *Submission to Australian Government Treasury's consultation on the use of Standard Business Reporting for financial reports – options paper*.

XBRL US 2016, *Context dates after period end date*, xbrl.us/data-rule/dqc_0005/ (accessed 25 June 2025).

—— 2019, *Element values are equal*, xbrl.us/data-rule/dqc_0004/ (accessed 25 June 2025).

Xero 2025, *Connect your bank to Xero: save time with bank feeds*.