Australian Government

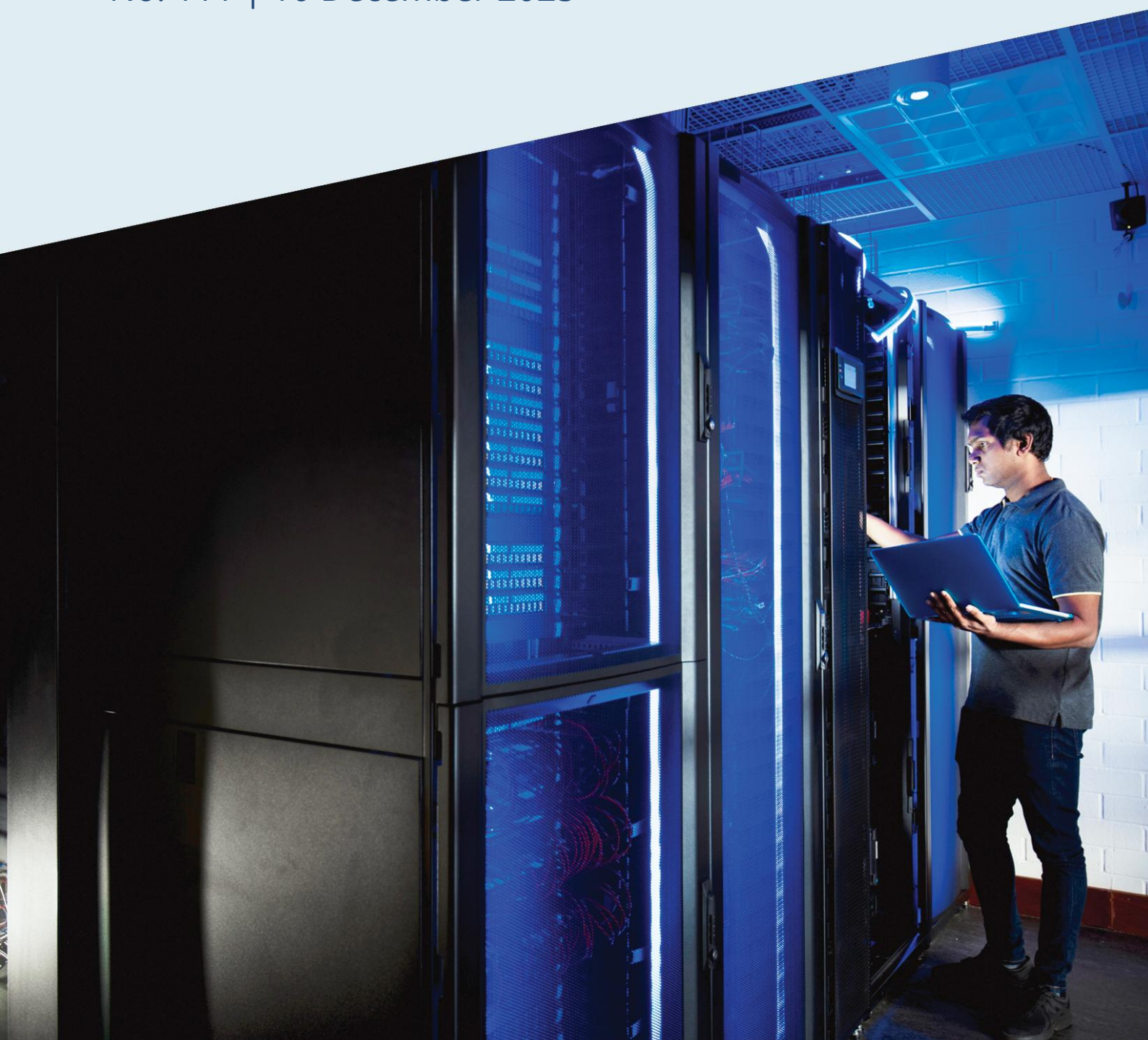**Productivity Commission**

pc.gov.au

Harnessing data and digital technology

Inquiry report

No. 111 | 10 December 2025

Acknowledgement of Country

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.

About us

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

Australian Government
Productivity Commission

Canberra Office

4 National Circuit

Barton ACT 2600

GPO Box 1428

Canberra City ACT 2601

Telephone 02 6240 3200

Melbourne Office

Telephone 03 9653 2100

www.pc.gov.au

10 December 2025

The Hon Dr Jim Chalmers MP
Treasurer
Parliament House
CANBERRA ACT 2600

Dear Treasurer

In accordance with section 11 of the *Productivity Commission Act 1998*, we have pleasure in submitting to you the PC's final report for the *Harnessing data and digital technology* inquiry.

Yours sincerely

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

Contents

Executive summary

Data and digital technologies are the modern engines of economic growth. Australia needs to harness the consumer and productivity benefits of data and digital technology while managing and mitigating any 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.

Emerging technologies like artificial intelligence (AI) could transform the global economy and speed up productivity growth. The Productivity Commission considers that multifactor productivity gains above 2.3%, and labour productivity growth of about 4.3%, are likely over the next decade, although there is considerable uncertainty. But poorly designed regulation could stifle the adoption and development of AI. Australian governments should take an outcomes-based approach to AI regulation – using our existing laws and regulatory structures to minimise harms (which the Australian Government has committed to do in its *National AI Plan*) and introducing technology-specific regulations only as a last resort.

Developing and training AI models is a global opportunity worth many billions of dollars. Currently, gaps in licensing markets – particularly for open web material – make AI training in Australia more difficult than in overseas jurisdictions. However, licensing markets are developing, and if courts overseas interpret copyright exceptions narrowly, Australia could become relatively more attractive for AI development. As such the PC considers it premature to make changes to Australia's copyright laws.

Data access and use fuels productivity growth: 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 GDP. The Australian Government should rightsize the Consumer Data Right (CDR) with the immediate goal of making it work better for businesses and consumers in the sectors where it already exists. In the longer term, making the accreditation model, technical standards and designation process less onerous will help make the CDR a more effective data access and sharing platform that supports a broader range of use cases.

The benefits of data access and use can only be realised if Australians trust that data is handled safely and securely to protect their privacy. Some requirements in the Privacy Act constrain innovation without providing meaningful protection to individuals. And 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 its spirit. The Australian Government should amend the Privacy Act to introduce an overarching outcomes-based privacy duty for regulated entities to deal with personal information in a manner that is fair and reasonable in the circumstances.

Financial reports provide essential information about a company's financial performance, ensuring transparency and accountability while informing the decisions of investors, businesses and regulators. The Australian Government can further spark productivity by making digital financial reporting the default for publicly listed companies and other public interest entities while also removing the outdated requirement that reports be submitted in hard copy or PDF form. This would improve the efficiency of analysing reports, enhance integrity and risk detection, and could boost international capital market visibility for Australian companies.

1

Recommendations

Artificial intelligence

Recommendation 1.1

Productivity growth from AI should be enabled within existing legal foundations. Gap analyses of current rules need to be expanded and completed

Any regulatory responses to potential harms from using AI should be proportionate, risk based, outcomes based and technology neutral where possible.

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

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

All reviews of the legal 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.

Recommendation 1.2
AI-specific regulation should be a last resort

AI-specific regulations should only be considered as a last resort and only for use cases of AI where:

- existing regulatory frameworks cannot be sufficiently adapted to handle AI-related harms
- technology-neutral regulations are not feasible or cannot adequately mitigate the risk of harm.

This includes whole-of-economy regulation such as the EU AI Act and the Australian Government's previous proposal to mandate guardrails for AI in high-risk settings.

Copyright and AI

» **Recommendation 2.1**
A review of Australian copyright settings and the impact of AI

The Australian Government should monitor the development of AI and its interaction with copyright holders over the next three years. It should monitor the following areas:

- licensing markets for open web materials
- the effect of AI on creative incomes generated by copyright royalties
- how overseas courts set limits to AI-related copyright exceptions, especially fair use.

If after three years the monitoring program shows that these issues have not resolved, the government could establish an Independent Review of Australian copyright settings and the impact of AI. The Review's scope could include, but not be limited to, consideration of whether:

- copyright settings continue to be a barrier to the use of open material in AI training, and if so whether changes to copyright law could reduce these barriers
- copyright continues to be the appropriate vehicle to incentivise creation of new works and if not, what alternatives could be pursued.

Data access

> **Recommendation 3.1**
> **Rightsize the Consumer Data Right**
>
> The Australian Government should commit to reforms that will enable the Consumer Data Right (CDR) to better support data access for high-value uses while minimising compliance costs.
>
> In the short term, the government should continue to simplify the scheme by removing excessive restrictions and rules that are limiting its uptake and practical applications in the banking and energy sectors. To do this the government should:
>
> - within the next two years, enable consumers to share data with third parties and simplify the on-boarding process for businesses
> - commit to more substantiative changes to the scheme (in parallel with related legislative reforms), including aligning the CDR's privacy safeguards with the Privacy Act and enabling access to selected government-held datasets through the scheme.
>
> In addition to the above, the CDR framework should be significantly amended so that it has the flexibility to support a broader range of use cases beyond banking and energy, by making the accreditation model, technical standards and designation process less onerous.

Privacy regulation

> **Recommendation 4.1**
> **An outcomes-based privacy duty embedded in the Privacy Act**
>
> The Australian Government should amend the *Privacy Act 1988* (Cth) to embed an outcomes-based approach that enables regulated entities to fulfil their privacy obligations by meeting criteria that are targeted at outcomes, rather than controls-based rules.
>
> This should be achieved by introducing an overarching privacy duty for regulated entities to deal with personal information in a manner that is fair and reasonable in the circumstances.
>
> The Privacy Act should be further amended to outline several non-exhaustive factors for consideration to guide decision-makers in determining what is fair and reasonable – including proportionality, necessity, and transparency. The existing Australian Privacy Principles should ultimately be phased out.
>
> Implementation of the duty should be supported through non-legislative means including documentation such as regulatory guidance, sector-specific codes, templates, and guidelines.
>
> The Office of the Australian Information Commissioner should be appropriately resourced to support the transition to an outcomes-based privacy duty.

Digital financial reporting

Recommendation 5.1
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 annual and half-yearly financial reporting mandatory for disclosing entities. The requirement for financial reports to be submitted in hard copy or PDF form should be removed for these entities. The implementation of mandatory digital financial reporting should be phased, with the Treasury determining the appropriate timelines for this approach.

Setting requirements for report preparation

The existing International Financial Reporting Standards (Australia) (IFRS AU) taxonomy should be used for digital financial reporting. The Australian Securities and Investments Commission (ASIC) should continue to update the taxonomy annually.

ASIC should be empowered to specify, from time to time, the format in which the reports must be prepared. At present, ASIC should specify inline eXtensible Business Reporting Language (iXBRL) as the required format.

Establishing infrastructure and procedures for report submission

ASIC, together with market operators such as the Australian Securities Exchange, should determine where and how digital financial reports are submitted. The arrangements should aim to minimise preparers' reporting burden while keeping reports accessible to report users.

Supporting the provision of high-quality, accessible digital financial data

ASIC should implement the measures necessary to ensure that digital financial reports contain high-quality data. ASIC could (among other actions):

- establish a data quality committee that would develop guidance and rules to improve data quality
- integrate automated validation checks into the submission process
- set guidelines around the use of taxonomy extensions and report format
- maintain feedback loops with stakeholders.
- To enable report users to harness the benefits of digital financial data, digital financial reports should be publicly and freely available, and easily downloadable.

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, 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 (appendix B).

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 its survey of the international literature, the OECD found that data sharing 'is estimated to generate 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' (OECD 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*.

In August 2025, we released an interim report outlining several reform options for consultation – we received more than 700 submissions in response to our interim report.

This final report makes recommendations across several policy areas that would 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. Chapter 2 deals with the potential issues AI may cause for copyright law, and the balance this legal framework attempts to strike between encouraging the production of new creative content and disseminating and using this content.
- Data about individuals and businesses underpins growth and value in the digital economy. While data access for consumers is inconsistent across the economy, data markets are evolving to better serve consumer demands. Our **data access** reform is focused on how the Australian Government can optimise the Consumer Data Right (CDR). Chapter 3 sets out short-term changes to make the CDR easier and cheaper to access for Australian consumers and businesses in the sectors where it already operates, and what additional changes are required to give it the potential to function as an economy-wide scheme in the longer run.
- 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 4.
- The adoption of **digital financial reporting** would increase the efficiency and accuracy with which the information in financial reports 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 5.

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.

Figure 1 – Four reform areas to support productivity growth

Higher productivity

Better decision making and efficiency

More innovation

Increased competition and investment

Enhanced data useability

Improved digital technology

Reduced regulatory compliance costs

Proportionate AI policy

Right sizing data access

Flexible privacy regulation

Digital financial reporting
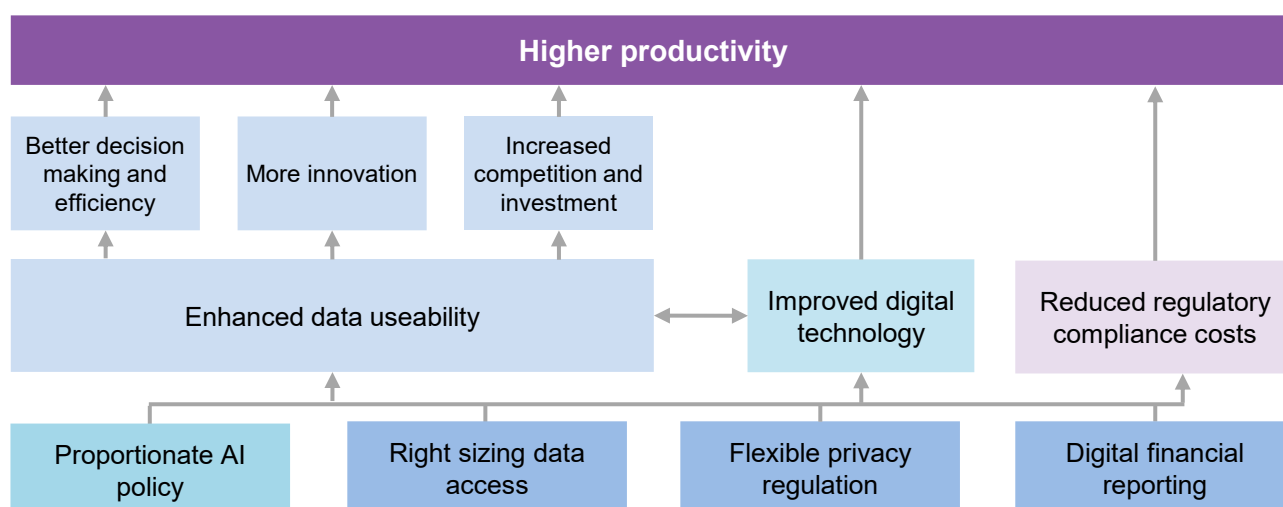
Box 1 – What makes data unique?

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.

Broad rights

The **data holder** has a de facto ability to control access and use

The **copyright holder** (author) has broad rights to control access and use

In general, broad rights to (control) access and use are **unassigned** (public domain)

In some cases, the right to (control) access and use is assigned to **private parties**

e.g. laws about confidentiality, intellectual property laws (patents)

DATA

Form

Information

Modifying rights (and obligations)

Some parties have limited rights to access and use

e.g. the Consumer Data Right provides for access to consumer data

Some parties have access rights

e.g. under Freedom of Information laws, privacy laws

Some parties have rights that limit access and use by others

e.g. privacy law provides protections for individuals

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.

Box 1 – What makes data unique?

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 has both upside and downside 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. At the same time, getting regulatory settings wrong could stifle AI investment without improving outcomes.

* Existing regulations are the starting point as many of the harms are already covered by existing regulation. Governments are conducting gap analyses to assess whether existing regulations sufficiently address all 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 legal frameworks or introduce technology-neutral regulations to adequately address the risk.

  • Before undertaking AI-specific regulation, governments should identify a clear gap in existing legal frameworks that cannot be addressed with technology-neutral solutions.

* The PC welcomes the Australian Government's *National AI Plan*'s emphasis on using Australia's existing, robust, largely technology-neutral legal frameworks as the foundation for addressing challenges associated with AI and other emerging technologies. This approach will best support Australia's ability to grasp the AI opportunity by building trust in the Australian community and providing regulatory certainty for firms.

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.[1] As AI continues to develop and its uses become clearer, the potential upside productivity benefits 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 estimate, 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 Gross Domestic Product (GDP) (2023-24 prices) over the next decade. Even a 0.5% multifactor productivity gain (the lower end of estimates produced by other studies) would be associated with a sizeable increase in economic activity – about $26 billion in additional GDP (2023-24 prices) 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 in the economy and could be leveraged for completely new applications (Filippucci et al. 2024, p. 17).

However, some productivity benefits may go unmeasured in the economic statistics. 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 tends to be underestimated in official economic 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 than official measures 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).

---

[1] For example, law firms use Large Language Models (LLMs) for evidence review and preliminary drafting (Snowden 2025a, 2025b) 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); and 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).

How AI could boost productivity

AI technologies can be applied in many different parts of the economy.

AI can help **automate** or **augment** a variety of tasks. Automation is when machines perform tasks that were previously performed by humans, while augmentation is where machines enhance rather than replace human roles. Both can free up skilled labour for tasks that add more value. This can affect employment, incomes, workloads, and leisure time in a number of ways depending on whether the time saved is recouped by workers, redeployed to other tasks, taken as a cost reduction, or put towards higher quality and quantity of production (JSA 2025b, p. 15).

Capital productivity can also be improved by AI. Rather than causing machines to replace people, in some cases, AI causes better machines to replace old machines or makes the old machines more efficient. For example, 'predictive maintenance' makes use of AI-powered smart sensors to detect wear and tear in various machines, resulting in a 30-40% reduction in downtime and a 20-30% reduction in maintenance costs (Ahuja and Gupta 2024, p. 291).

AI could also lead to the **emergence of new occupations**, which could either be a novel combination of existing tasks or involve tasks that did not previously exist. This could increase productivity if these new occupations lead to more valuable use of labour.

In some cases, the use of AI could **improve allocation and participation in the labour market as well**. Greater use of AI could enable marginalised groups to join the workforce. A study by the Organisation for Economic Co-operation and Development (OECD) identified 142 examples of AI-powered tools that could support people with disability in the labour market (2023, p. 8). Examples include a text simplification program to help workers with learning disabilities, and a combined image recognition and text to speech application to assist people with low vision (2023, p. 80).

Over time, AI could also lead to the emergence of **new products and services**. This could include new technology-based services, or new ways of using existing ones. These adaptations are difficult to predict or anticipate, but by their nature are likely to have wide-ranging implications compared to the application of AI to existing tasks and occupations.

AI could also **affect the pace of innovation** by speeding up scientific progress, leading ultimately to faster economic growth.[2] AI has already been applied in medical and health research, biology and biochemistry (Charley 2024; Devlin 2025; ScienceDaily 2024).

AI is already changing Australian workplaces

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

- *Repetitive administration tasks* – AI tools are being used to save time on various administrative tasks such as drafting emails, responding to customer inquiries or scheduling activities (ADHA, qr. 16, p. 8; Marrickville Legal Centre, qr. 38, p. 3; MFAA, qr. 67, p. 3; Osjavi Rana, qr. 68, p. 3; TCA, qr. 69, p. 4).

---

[2] 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.

- *Creative sector and media applications* – film makers, game designers and design tool producers have all used AI to develop visual effects and simplify different stages of media and art production (Adobe, sub. 307, pp. 1-2; Ausfilm, sub. 528, p. 3; Australian Film/TV Bodies, sub. 541, p. 2; IGEA, sub. 313, p. 2).[3]
- *Education and training* – educators are using a variety of AI tools are being to augment their teaching (AHEIA, sub. 358, p. 1; The University of Sydney, qr. 21, p. 6; RUN, qr. 22, pp. 3–4; CAG TAFE, qr. 41, p. 3).
- *Customer service and retail* – businesses are using AI chatbots to provide 24/7 customer service, augment call centre staff and personalise some services (AFIA, sub. 565, p. 7; Bunnings Group, sub. 128, p. 2; Lite n Easy, sub. 144, p. 2; NAB, sub. 581, p. 18).
- *Heavy industry operations* – the mining sector in particular is using AI to operate autonomous trucks, trains and drills, analyse satellite imagery and geological data, and predict equipment maintenance needs (CME, sub. 386, p. 3; MCA, sub. 590, p. 15)
- *Software and Information Technology systems* – some participants are using AI tools and processes to develop software or for internal cybersecurity purposes (Atlassian, qr. 50, p. 6; Microsoft, qr. 52, pp. 4–5; Montu Group Pty Ltd, qr. 35, p 3; Salesforce, qr. 57, pp. 3–4).
- *Health services* – AI is being used for a range of administrative and clinical purposes (MSIA, qr. 70, p. 3). Nurses are using AI-enabled decision support and digital documentation tools (ACN, sub. 549, p. 14), while pathologists and researchers are using AI to detect and grade disease severity and identify changes in the tissues to model prognoses or responses to treatments (qr. 33, pp. 2-3).

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 sort fruit based on how ripe it is (Field 2025). The Commonwealth Bank of Australia stated that it has seen a 30% drop in customer-reported fraud due to measures like AI powered transaction alerts (Commonwealth Bank of Australia 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 and catalogue new Aboriginal rock art sites from photos (Richards 2023). Manually cataloguing rock art is otherwise highly labour intensive and time consuming, and without AI, many of these sites may have remained undiscovered. In the Northern Territory, AI analysis of drone footage is being used to identify discarded and drifting fishing nets (Ellis 2025). Rangers would otherwise have to visually inspect the coastline for these fishing nets themselves. While AI is being applied to a broad range of tasks, the overall effect of AI on the job market – how many jobs will be changed, gained or lost – is highly uncertain (box 1.2).

Box 1.2 – How will AI change the mix of roles people work in?

AI, like all previous technological changes, is anticipated to increase the demand for some skills and professions and decrease it for others, leading to both new opportunities and difficult transitions. But which occupations will be affected, the amount of job losses, job creation and job changes, and the speed of the transition are uncertain.

Just because an occupation is highly 'exposed' to AI does not necessarily mean there will be significant job losses (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 tasks performed by

---

[3] The interaction between AI and copyright law is discussed in chapter 2.

Box 1.2 – How will AI change the mix of roles people work in?

humans. Even when AI automates jobs, other factors can balance out the impact. For instance, AI might lower the cost of production in a certain industry. This could lead to lower prices, which encourages people to buy more products from that industry. 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 increase the net number of jobs, but potentially displace some workers.[a] If AI does displace a significant number of workers, the Australian Government may need to consider specific supports for retraining them, in addition to existing unemployment assistance.

Jobs and Skills Australia, the Australian Government body responsible for advising on future workforce needs, released a *Gen AI Capacity Study* in August 2025, which examined how generative AI may affect the structure of the Australian workforce. The report found that for most occupations, AI has a greater likelihood of 'augmenting' a task than it does 'automating' it. Despite this, modelling presented in the Jobs and Skills Australia report still predicted that AI would initially lead to job losses, before supporting additional job creation (compared to a scenario of no AI).

a. For example, a report by the World Economic Forum forecasted, at a global level, a net growth of about 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). When considering broader data and digital development (including AI technology) through to 2030, the World Economic Forum projected 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 related to AI development, 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).

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

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 address risks* – consistent and reliable regulation can help promote trust (and trustworthiness) in AI technology, which in turn makes business more willing to invest in, develop, and adopt AI. Similarly, in addition to directly regulating AI, regulation generally, including in labour, electricity and water markets, as well as in construction and zoning, should also be designed, among other things, to minimise market distortions and have benefits that outweigh costs to support the efficient adoption of AI.[4]
- *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 its uptake.
- *Building foundational capabilities to support AI uptake* – governments play a major role in regulating and funding education and training in Australia (PC 2025a). As a result, governments will partly determine whether these systems can provide the skills necessary for effective AI use.

---

[4] There are many guides to good regulation. Here the PC has used OECD's (OECD 2005, p. 3) list of seven principles for designing good regulation.

- *Investing in internet 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.

We have chosen to focus this chapter on government regulation for several reasons including: the lack of international consensus on the best way to regulate AI; calls from industry for more certainty on future AI regulation; the overlap of some of these above areas with other inquiries running parallel with this one (such as the inquiry into *Building a skilled and adaptable workforce* (PC 2025a)), and contemporary Australian Government proposals for the regulation of AI in Australia. We are particularly interested in the direct regulation of AI. But as above, we note the importance of fit-for-purpose regulations that minimize market distortions and have benefits that outweigh costs.

The PC notes that the Australian Government has announced a National AI Plan to 'harness AI technologies to create a fairer, stronger Australia' (DISR 2025a, p. 5). This plan centres on three policy objectives for AI:

- capturing the opportunity – capturing the economic benefits of offered by AI
- spreading the benefits – ensuring that the economic gains are equitably distributed
- keeping Australians safe – mitigating the risk of harm from AI use (DISR 2025a, p. 7).

To achieve these objectives the Australian Government has also announced a set of policy actions, some already underway. The Australian Government has also announced an intention to further a set of 'data centre principles' where, in return for projects meeting sustainability targets, the Australian Government will attempt to coordinate the data centre approval process in conjunction with lower levels of government (DISR 2025a, p. 9,11).

Mitigating the potential downside risks of AI

AI, like all previous technological developments, comes with upside and downside risks. On the downside, AI has the potential for misuse, malfunction and unintended consequences leading to harm. Policymakers need to mitigate the downside risks without undermining 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 offences 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 research and development capability, market concentration or single points of failure, environmental risks, privacy risks and copyright risks (Bengio et al. 2025, pp. 17–20).

Participants told the PC they were concerned about the potential for AI to cause harm in a variety of ways.

- Mistakes and hallucinations – mistakes by AI applications in 'high risk' scenarios such as health care, financial services, law enforcement or employment could have disproportionate effects (ADHA, qr. 16, p. 9; Cancer Council Australia, qr. 64, pp. 7–8; PHRN, sub. 603, p. 2; Salesforce, qr. 57, p. 5).
- Bias and discrimination – the output of an AI model reflects its training data. Where training data is biased, perhaps because some population groups are not sufficiently represented, AI may discriminate (Cancer Council Australia, qr. 11, p. 7; Endpoint Strategy, sub. 342, p. 2; EY Australia, qr. 27, p. 8; MCRI, qr. 34, p. 6; BSA, qr. 73, p. 8; EFA, sub. 288, p. 8).
- Emissions – AI is computationally intensive and could contribute to higher emissions due to energy use (APDG, qr. 6, p. 5; ATN Universities, qr. 13, p. 3; ASCA, qr. 14, p. 7; CA ANZ, sub. 560, p. 17; Endpoint Strategy, sub. 342, p. 1; Terri Janke and Company, sub. 436, pp. 6-7).

- Threats from harmful actors – AI's ability to generate content quickly could make it easier for people to commit harmful acts, such as terrorist attacks or the manipulation of children (Alannah & Madeline Foundation, sub. 119, p. 7; Digital Child, sub. 379. pp. 4, 6; Good Ancestors Policy, qr. 5, p. 4; ICMEC, sub. 416, pp. 2-3).
- Lack of understanding of AI – the pace of AI development may be outstripping regulators' ability to mitigate associated risks (ADHA, qr. 16, p. 9; Good Ancestors Policy, qr. 5, pp. 3-5).

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. Issues like the environmental pressures posed by high energy demands, or even the potential issue of copyright infringement (chapter 2), are not unique to AI and continue trends seen in previous phases of technological development.

That said, AI can shift the economic incentives in ways that exacerbate existing problems. For example, people can use AI to perform antisocial tasks much more cheaply and at a greater scale than they could previously. This has made issues like deepfake imagery or manipulation of public opinion by malicious actors – which have existed for a long time – much more significant.

An example some participants raised of AI exacerbating an existing risk of harm is with respect to the current requirements to consult employees about major changes in the workplace (box 1.3).

Regulators and policymakers should focus on mitigating the *additional risk* of these harms occurring, rather than treating them as wholly new problems.

Box 1.3 – Some participants are concerned about the level of consultation for the use of AI in the workplace

Some participants in 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 changes that are 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. There is ongoing debate about the adequacy of these provisions for AI. Employee representatives have argued that section 205 is insufficient in dealing with the use of AI in the workplace (ACTU, sub. 575, pp. 13-14. UWU, sub. 520, pp. 20-21); employers counter with the opposite view (ACCI 2025; BCA 2024, pp. 12–13).

Unnecessarily 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 that government pursues any regulatory goal at lowest possible cost.

There are real world examples of regulations having an unintended chilling effect on innovation. The European Union's General Data Protection Regulation aims to protect the data rights of individuals but appears to have stifled innovation and investment (box 1.4).

Box 1.4 – 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). 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). 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 been 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.

The mere threat of regulation can hinder innovation if firms believe it may be too onerous, or its direction is uncertain. Firms can hold off on investing into emerging technologies if they are concerned that forthcoming regulations will make it financially unviable to use them.

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

- The AIIA 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 (qr. 49, p. 6).
- MYOB 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 previously proposed mandatory guardrails. 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 (qr. 31, pp. 5–6).

• Montu stated that regulatory uncertainty about AI has created 'hesitancy in adoption, as guidelines and liability frameworks remain unclear'. It added that its '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 (qr. 35, p. 3).

Australia's business AI adoption and investment rates compare relatively poorly internationally (the US is the recipient of by far the highest level of investment), though it is uncertain how strongly this relates to policy settings (box 1.5).

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

The evidence on Australia's overall AI uptake shows a mixed picture. Within Australia, individuals and large firms are adopting and investing heavily in AI tools while small businesses seem to be moving much slower. Overall, Australian businesses appear to be embracing AI less quickly than their international peers. Given that AI adoption can require significant business investment, Australia's generally low rate of business investment may partially explain this (PC 2025b). To the extent that the economic benefits of AI depend on business adoption, this is a potentially concerning portend for future productivity growth.

Research by Jobs and Skills Australia found that many large Australian firms are investing heavily in AI. It found that in 2024, 'the vast majority of ASX200 mentioned technology investments in their annual reports', and that 57% of these mentioned AI-related investments. Those that did mention investments in AI represented 77% of Australian Stock Exchange market capitalisation (JSA 2025b, p. 34).

Jobs and Skills Australia found that investment by these firms in AI focused on improving interactions with customers (such as by integrating chatbots and customer insights tools), streamlining internal processes and reducing manual tasks, and creating new products or new features for existing products.

Small-sized and medium-sized businesses appear to be adopting AI at lower levels than larger businesses. The National AI Centre's AI Adoption tracker showed that in the first quarter of 2025, 82% of firms with 200-500 employees had adopted AI, compared with just 33% of firms with 0-4 employees (NAIC 2025).

In terms of how Australian adoption rates compare to other countries, the evidence is more preliminary than definitive. Nonetheless, studies so far indicate that while individuals are using AI at similar rates to peer nations, business adoption is lagging.

• 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 the 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

> **Box 1.5 – Is Australia already lagging in AI take-up?**
>
> '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 demand growth for people with AI skills was 36%
>   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 comparatively slower adoption in
>   Australia, or if adoption has already matured and growth is slower as a result.
> - Stanford University's AI index used LinkedIn data to show that Australia's relative AI skill penetration
>   was slightly below the global average. It also ranked Australia with the United States, Germany and
>   Great Britain as the least optimistic for AI sentiment (Stanford HAI 2025, pp. 235, 401). The index also
>   shows Australia performs relatively poorly on AI patents, which is consistent with the country's
>   generally low rate of patenting.

The PC's blueprint for AI regulation

Identifying and remedying gaps in current regulation posed by AI must come first

The range of commonly cited AI risks span several Australian Government portfolios including health, consumer protection, criminal law, national defence, financial regulation, media regulation and intellectual property. 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 legal and regulatory frameworks.

Gap analysis 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 is occurring, or is likely to occur, in the absence of AI
- 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 the regulation, or improvements to its enforcement, are required (figure 1.1).

Gap analyses should be conducted by the relevant government agency or regulator with existing expertise in the use cases that are likely to lead to harm. Agencies and regulators should work in close collaboration with relevant policymaking agencies, including the newly established AI Safety Institute (AISI) (discussed further below) to ensure a consistent, coordinated and transparent whole-of-government approach. Consultation with consumer and industry stakeholders as well as experts in the field will be essential. These gap analyses would encompass most areas of civil and criminal law. As an example, the Therapeutic Goods Administration (TGA) has conducted a review on, among other things, the continuing appropriateness of their existing regulatory approach and requirements for medical devices that incorporate AI (TGA 2024, 2025a).

Government should complete these AI gap analyses urgently. They should do this before considering any overarching AI regulations, such as the Australian Government's previous proposal to mandate guardrails for AI in high-risk settings (below). Creating overarching, economy-wide regulations before identifying the gaps

in existing legal frameworks risks duplication and unnecessarily high compliance burden with little benefit. The PC welcomes the Australian Government's recently released *National AI Plan* and in particular its focus on using Australia's 'strong existing, largely technology-neutral legal frameworks' to mitigate AI harms, as opposed to, in the first instance, introducing new, overarching AI regulation (DISR 2025a, p. 28).

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

Where could there be gaps?	• Are existing legal frameworks adequate? Does AI highlight the framework's existing flaws? • How will the nature of AI challenge or prevent effective enforcement? • How might automation displace existing legislation focused on workers or operators? • What new forms of harm may be introduced?
When these are answered, it is time to consider further questions	
Can existing legal frameworks bridge the gap?	• Could existing laws and legal frameworks be clarified or amended? • How can existing frameworks, processes or institutions be leveraged? • Can regulators' capabilities be strengthened?
When new laws are still needed there are important considerations	
What new laws might be needed?	• New laws should have net benefits compared to real-world counterfactuals. • New laws should be technology neutral. • Where legal frameworks diverge globally, Australia should minimise additional requirements compared to those in major economies and actively participate in international forums.

Agencies are already taking the lead in undertaking gap analyses

In the 2024-25 Budget, the Australian Government allocated just under $40 million over five years to the development of policies and capability to support the safe and responsible adoption and use of AI, including work to clarify and strengthen existing laws (Treasury 2025c, p. 3). A number of AI-focused regulatory gap analyses resulted from this allocation.

The PC is aware the Australian Government Department of Health and Aged Care (2024), the TGA (2024) and the Australian Government the Treasury (2025c) have completed AI-focused regulatory gap analyses.

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). The Attorney General's Department (2023a) has an ongoing Copyright and Artificial Intelligence Reference Group which has a stated goal to ensure copyright law keeps pace with the challenges posed from AI (chapter 2).

The TGA review is a particularly rigorous example of a gap analysis that could be used as a template for future gap analyses. Box 1.6 summarises the TGA review to illustrate the types of issues that a robust gap analysis should consider as a minimum.

Box 1.6 – The TGA's gap analysis could be used as a template for future reviews

In 2025, the Therapeutic Good Administration undertook a targeted review of legislation, which found the 'existing legislative framework is largely appropriate for the increasing use of AI in therapeutic goods' (TGA 2025b, p. 5). Public consultation was held, and the review process was also mapped to the mandatory guardrails work. However, broader policy considerations related to AI were not a focus of this work. Outcomes were grouped across findings in legislation, regulations, legislative instruments, guidance and international harmonisation (TGA 2025b, p. 6). Many findings stated that further review and consultation were required to determine if certain definitions and responsibilities were appropriate, or to specify the changes needed (TGA 2025b, pp. 8–19). Given that the legislative review element of the report focused on one piece of legislation[a], the findings could easily be linked to the instruments that required review. The Therapeutic Good Administration also proposed further targeted consultation on regulatory refinements during 2025 and 2026 (TGA 2025b, p. 5).

Other features that gap analyses could include in order to be targeted and effective are:

- detail on how different aspects of the regulatory framework already interact with AI related harms
- outlining which specific AI risks or harms need to be addressed through any changes recommended
- specific information on what types of changes should be considered if further or ongoing review is recommended
- some detail on the steps that need to be taken if further review is required, such as who may be best suited to do it, and if there are other related government processes underway.

a. Chapter 6 of the *Therapeutic Goods Act 1989* (Cth) outlines the Therapeutic Good Administration's role and responsibilities.

Source: Therapeutic Goods Administration (2025b).

» **Recommendation 1.1**
Productivity growth from AI should be enabled within existing legal foundations. Gap analyses of current rules need to be expanded and completed

Any regulatory responses to potential harms from using AI should be proportionate, risk based, outcomes based and technology neutral where possible.

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

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

All reviews of the legal 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.

Technology-specific regulation should be a last resort

Australian governments should first seek to identify, and where possible, address gaps in legal and regulatory frameworks created by the increased use of AI. Where the risk of harm cannot be adequately mitigated by changes to existing legal frameworks, new laws could be considered. In this context, the PC is using 'regulation' and 'legal changes' synonymously to mean any addition to the existing legal system including all aspects of civil and criminal law. New laws should be **technology neutral**, create a **net benefit** compared to the status quo, and (where possible) **minimise divergences** between Australian and overseas regulatory structures.

The importance of technology neutrality

Technology-neutral regulation allows regulators to focus on the risk of harm itself (for example, employers discriminating against job applicants) rather than particular *means* of causing harms (for example, an employer recklessly using AI in a way that discriminates against job applicants). Such an approach means that regulations will remain relevant as technology changes – AI may not be the end of information communication technology innovation and new technologies may pose similar risks. Moreover, technology-specific regulation can create loopholes where the risk of harm is only regulated when a particular technology is used. Technology-specific regulation also distorts the incentive to use new technology, potentially without reducing the risk of harm where the new technology is not the only activity leading to the risk of harm.

The PC recognises that technology-neutral regulation is not always feasible or able to adequately mitigate risk of harm. For example, the Australian Government directly regulates the importation of motor vehicles. It does this by requiring vehicle models to meet 'Australian Design Rules' before they can be imported and hence driven on Australian roads (such as Vehicle Standard (Australian Design Rule 42/05 – General Safety Requirements) 2018). In this case, the Australian Government has made the judgement that technology-neutral approaches would not be sufficient to mitigate the risk of harm stemming from vehicle design defects or malfunctions.

For any particular type of harm, the threshold question is whether existing regulatory frameworks or new technology-neutral regulation can adequately and feasibly mitigate the risk of harm stemming from an individual using AI. AI-specific regulation should be a last resort.

Consistency with overseas AI frameworks complicated by a lack of consensus

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. These are good reasons for Australia to be a 'regulation taker' in the context of international AI regulation: to ensure its AI regulations are consistent with international standards (PC 2024b, p. 9).

However, the PC reviewed the regulatory stance towards AI in the 38 OECD countries (table 1.1, appendix D) and found, at present, there appears to be no international consensus on how to approach AI regulation.

Almost half do not have AI-specific regulation or have regulation that has been introduced to the legislature that has yet to pass (countries that account for 49% of GDP in the OECD). The United States of America is the most prominent country to have not introduced AI-specific regulation (at the federal level), though some US states have implemented AI-specific legislation (such as California). Australia and New Zealand are both yet to introduced broad-based technology-specific regulation to their legislatures.

Countries with broad-based AI-specific regulation account for about 35% of total GDP in the OECD. The European Union is the main jurisdiction that has enacted broad-based regulation, with its EU Artificial Intelligence Act (Regulation (EU) 2024/1689).

Table 1.1 – No consensus approach to AI regulation

AI-specific legislation status in OECD countries[a]

Legislation status	Jurisdiction	Cumulative share of OECD GDP[c]
No legislation		49%
No legislation introduced to parliament or passed	Australia, Iceland, Israel, New Zealand, United States – Federal	(28%)
Regulation introduced to parliament (over 12 months ago) but not yet passed	Canada[b], Chile, Costa Rica, Mexico, Turkiye	(13%)
Regulation introduced to parliament (less than 12 months ago) but not yet passed	Colombia, Norway, Switzerland, United Kingdom	(8%)
Passed and narrow	Japan, United States – California, United States – Texas, United States – Utah	16%
Passed and broad-based	Austria[d], Belgium[d], Czechia[d], Denmark[d], Estonia[d], Finland[d], France[d], Germany[d], Greece[d], Hungary[d], Ireland[d], Italy[d], Latvia[d], Lithuania[d], Luxembourg[d], Netherlands[d], Poland[d], Portugal[d], Slovak Republic[d], Slovenia[d], South Korea, Spain[d], Sweden[d], United States – Colorado	35%

a. This table only includes bills that specifically govern AI use and development and look to minimise or remove AI-related risks. Many nations have passed other legislation that encourages investment in AI development. The list in the table is not exhaustive, and some bills designed to encourage investment may contain measures designed to set up future regulatory measures, institutions or reviews that look to mitigate AI-related risk. **b.** Canada introduced a bill in June 2022, but the passage of the legislation ended when all legislation in parliament was prorogued before the 2025 election (Duball 2025; Fraser and Anderson Dykema 2025). **c.** The GDP of the United States was apportioned to the various categories based on the regulatory stance of its states. Although the stance of the federal government of the United States of America is listed in the table, its GDP is only counted at the state level and so its federal status has no effect on the cumulative GDP share of each category. **d.** European Union member country.

Source: Relevant international legislation and bills iapp (2025), Ministry of Digitalisation and Public Governance (Norway) (2025), News Service Bund (2025). [5]

---

[5] Act on the Development of Artificial Intelligence and Establishment of Trust [Artificial Intelligence Basic Act] (Republic of Korea); Act on the Promotion of Research and Development, and Utilization of AI-related Technology, Act No. 53 of 2025 (Japan); Artificial Intelligence (Regulation), Bill [HL] 30 (United Kingdom); Bill C-27, Digital Charter Implementation Act, 2022 (Parliament of Canada); Colorado Revised Statutes Annotated, Title 6, Article 1, Part 17, Colorado Artificial Intelligence Act (State of Colorado); Council of Europe Framework on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, EU Artificial Intelligence Act (Regulation (EU) 2024/1689); Expediente 23.771: Ley de Regulación de la Inteligencia Artificial en Costa Rica [Law Regulating Artificial Intelligence in Costa Rica] (Costa Rica); Expediente 23.919: Ley para la Promoción Responsable de la Inteligencia Artificial en Costa Rica [Law for the Responsible Promotion of Artificial Intelligence in Costa Rica] (Costa Rica); Expediente 24.484: Ley para la Implementación de Sistemas de Inteligencia Artificial [Law for the Implementation of Artificial Intelligence Systems] (Costa Rica); Proyecto de Ley que regula los sistemas de Inteligencia Artificial [Bill regulating Artificial Intelligence systems] (Chile); Proyecto de Ley Nº 422 de 2025 Senado, "Por medio de la cual se establece el marco legal para la promoción, desarrollo y uso responsable de la inteligencia artificial en Colombia" [Senate Bill No. 422 of 2025, "Establishing the legal framework for the promotion, development and responsible use of artificial intelligence in Colombia"] (Colombia); Ley Federal para el Desarrollo Ético, Soberano e Inclusivo de la Inteligencia Artificial [Federal

Some countries that have introduced AI-specific regulation did so in relatively narrow contexts (accounting for 15% of GDP in OECD countries). For example, the US state of Texas has introduced AI regulation mainly focusing on the public sector with only some private sector AI-uses prohibited, such as developing AI with the intent of committing crimes (House Bill 149, Texas Responsible Artificial Intelligence Governance Act (State of Texas)). Japan has also introduced AI-specific regulation, but it appears to impose minimal responsibilities, and it does not include any enforcement measures.

A few countries have introduced AI-specific regulation to the legislature but the process appears to be in stasis. Canada 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 of December 2025 there is no new information on whether the Bill C-27 process will restart or if new legislation will be considered. The United Kingdom is in a similar position to Canada, having introduced a bill for AI-specific legislation to parliament in March 2025[6], but as of December 2025 the bill has yet to progress to a second reading (Courea and Stacey 2025).

Despite this lack of consensus among advanced economies on regulating AI, there are steps Australia could take to ensure the interoperability of its legislative frameworks. Australia should continue to be an active participant in international forums (for example, as part of its membership of the Bletchley Consensus[7]) 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 goals and support our productivity growth.

Whole-of-economy AI-regulation should only be considered after gap analysis

With the *National AI Plan*, the Australian Government has moved away from its previously proposed whole-of-economy, technology-specific AI regulation (that is, the proposal to mandate guardrails for AI in high-risk settings, box 1.7) to an approach that leverages Australia's existing legal frameworks to mitigate the risk of AI-related harm (DISR 2025a, p. 28).

The PC welcomes this move away from broad-based, technology-specific regulation as a first response. Whole-of-economy regulations discussed above such as those seen in the EU, being proposed in Canada or as previously proposed for Australia in the form of the mandatory guardrails for AI in high-risk settings, create regulatory uncertainty, which can stifle innovation. Whole-of-economy regulations are only justified where gaps in existing regulatory frameworks cannot be filled with technology-neutral laws.

Law for the Ethical, Sovereign and Inclusive Development of Artificial Intelligence] (Mexico); Yapay Zekâ Kanun Teklifi [Artificial Intelligence Bill] (Turkiye); Senate Bill 53 (Cal.), Chapter 138, Transparency in Frontier Artificial Intelligence Act (State of California); House Bill 149, Texas Responsible Artificial Intelligence Governance Act (State of Texas); Senate Bill 149, Artificial Intelligence Policy Act (State of Utah).

[6] The Artificial Intelligence (Regulation) Bill was a private members' bill that originated in the House of Lords, session 2024-26.

[7] The Bletchley Consensus is a shared framework for governing advanced AI. It is a global agreement that frontier AI poses cross-border risks and requires international cooperation, safety testing, and sharing an evidence-based understanding of risks. There are 28 signatory countries plus the EU, including the United States, United Kingdom, Australia, China, Japan, South Korea and India (DISR 2023).

> **»** **Recommendation 1.2**
> **AI-specific regulation should be a last resort**
>
> AI-specific regulations should only be considered as a last resort and only for use cases of AI where:
>
> - existing regulatory frameworks cannot be sufficiently adapted to handle AI-related harms
> - technology-neutral regulations are not feasible or cannot adequately mitigate the risk of harm.
>
> This includes whole-of-economy regulation such as the EU AI Act and the Australian Government's previous proposal to mandate guardrails for AI in high-risk settings.

Box 1.7 – The PC had concerns with the previous proposal to mandate AI guardrails

In August 2024, DISR released a set of ten voluntary AI safety standards, or 'guardrails', based on international risk management standards.[a] These were later condensed into six 'essential practices' in the *Guidance for AI Adoption* to help organisations apply the guardrails to their own contexts. In September 2024, the Australian Government released a proposals paper for a set of mandatory guardrails for AI in high-risk settings. The paper proposed turning the voluntary guidelines into mandatory regulations for AI development and application (DISR 2024b).[b]

The guardrails themselves were well-suited to their existing role as *voluntary* guidelines for safe model development and deployment. They outlined reasonable risk management processes, including model testing, risk planning, and transparency around data and copyright use. They represented a significant step in Australian AI governance, providing structured, internationally recognised standards – especially valuable for smaller businesses without formal risk procedures. Submissions to this inquiry and the mandatory guardrails consultation process noted that larger organisations already follow similar approaches.[c]

With respect to mandating the guardrails, the PC had three concerns with the proposal:

First, the mandatory guardrails applied to all high-risk uses of AI but ignored the role of existing regulation, or the option of new technology-neutral regulations, to mitigate risk. Gap analyses are needed to understand the role that existing or new technology-neutral regulations can play in mitigating risk and whether any remaining risks could appropriately be dealt with by whole-of-economy regulation.

Second, the proposal suggested classifying all general purpose AIs above an unspecified technical threshold as inherently high risk (DISR 2024b, p. 18). This could capture common generative AI tools like ChatGPT, Claude and Grok.

Third, the guardrails regulate **processes** – risk management, testing, and transparency – rather than **outcomes** and thus **do not directly prevent harm**. In many areas, such as medical devices regulated by the TGA (2025a, pp. 27–30), similar requirements already exist, so duplicating them would raise compliance costs without improving outcomes. While some stakeholders argued that mandating guardrails is necessary to enforce existing legal frameworks (HTI, sub. 344, p. 20; ADM + S, sub. 412, p. 10), this is not true for all laws. Determining where guardrails add value **requires a comprehensive gap analysis** to avoid duplication and ensure regulation is technology neutral.

a. DISR drew on 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 2024a, p. 5) in designing the voluntary guardrails for AI. **b.** The mandatory guardrails do differ from the

> **Box 1.7 – The PC had concerns with the previous proposal to mandate AI guardrails**
>
> 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 2024b, p. 35, 2024a, pp. iv, 13–14). **c.** Accenture (2024b, p. 3); Atlassian (qr. 50, p. 8); Commonwealth Bank of Australia (2024b, p. 3); IBM Australia (2024, p. 1); Indeed (2024, pp. 2–3); Intuit Australia (qr. 36, pp. 9-11); KPMG (qr. 60, p. 3), LinkedIn (2024, pp. 4–5); Mastercard (2024, p. 1); Microsoft (qr. 52, p. 5); RMIT University (2024, p. 1); Salesforce (qr. 57, p. 5); SEEK Limited (2024, pp. 3–4); Telstra (2024a, pp. 4–5); The University of Melbourne 2024 (2024, p. 3); Workday Australia (qr. 56, p. 6).

Are there risks of prioritising gap analyses ahead of technology-specific regulation?

Participants broadly supported the proposal for gap analyses in our interim report. At the same time, views diverged on the use of technology-specific regulation such as the Australian Government's previously proposed mandatory guardrails (box 1.8). Many raised concerns about the prospect of delaying the introduction of broader AI-specific regulation, given the potential for harms to occur.

> **Box 1.8 – Participant's views on mandatory guardrails were mixed**
>
> The PC heard a variety of views from inquiry participants with regard to the mandatory guardrails.
>
> Generally, business and industry groups favoured delaying mandatory rules until gap analyses were complete.[a] However, there was disagreement from other inquiry participants,[b] many of whom stated that the speed of AI development required dedicated legislation to protect the community from harms. Some participants were in favour of the draft recommendations on completing gap analyses, but expressed reservations about pausing the mandatory guardrails legislation or other forms of AI-specific legislation.[c]
>
> Some participants raised broader concerns related to the draft recommendations, stating that there was also a need for improvements to resourcing and governance arrangements. Australian Research Data Commons state that 'whilst regulatory reviews proceed and innovation accelerates, regulators require enhanced oversight capabilities and resources' (sub. 422, p. 4), while DIGI stated 'the Government, and specifically sectoral and horizontal regulators, be resourced to assess to what extent AI is already regulated within the scope of existing laws in all the sectors where AI will be applied' (sub. 759, p. 3).
>
> In their submission to this inquiry, ADM+S argued that an overarching piece of AI related legislation is required to enable existing legislation to tackle AI related harms. The complexity and opacity of AI systems and supply chains are stated as features of AI systems that make the 'application of any existing laws extremely difficult' (sub. 412, p. 10).
>
> **a.** AHEIA (sub. 358, p. 1); AIIA (sub. 301, pp. 2-3); Amazon (sub. 535, p. 10); BCA (sub. 488, p. 2); IPA (sub. 481, p. 1); MCA (sub. 590, p. 16); MSIA (sub. 487, p. 2); NAB (sub. 581, p. 18); TCA (sub. 534, p. 12); Wesfarmers (sub. 592, p. 22). **b.** ACTU (sub. 575, p. 12); Alannah & Madeline Foundation (sub. 119, p. 4); Digital Child (sub. 379, p. 4); DRW (sub. 311, p. 8); EFA (sub. 288, p. 2); Global Shield Australia (sub. 329, pp. 8-9); Good Ancestors (sub. 169, p. 5); Governance Institute of Australia (sub. 28, p. 6); ICMEC Australia (sub. 416, pp. 3-4); MEAA (sub. 466, p. 4); SRI4GoodAI (sub. 206, pp. 1-2); Terri Janke and Company (sub. 436, p. 3); UNSW.ai (sub. 133, p. 1); UWU (sub. 520, p. 21). **c.** ARDC (sub. 422, p. 4); Free TV Australia (sub. 770, p. 8); Law Council of Australia (sub. 599, pp. 9).

First, it is important to note that gap analyses will play a significant role in ensuring effective protections against the new and heightened risks associated with AI technologies. Leveraging and amending current legal and regulatory frameworks is a critical step toward coherent and effective regulation. Ensuring existing laws are properly applied is a matter of urgency.

Second, the gap analyses are critical to informing the design of and need for any technology-specific AI regulation, including the previously proposed mandatory guardrails. The Human Technology Institute recommended that 'coordinated reform to priority areas of existing law – guided by an expedited, high-level gap analysis' should be conducted 'in parallel to the mandatory guardrails process' (HTI, sub. 344, p. 27). Even if this was to occur, it is important to acknowledge that the mandatory guardrails – if they had gone ahead as proposed in October 2024 – would have been designed without the benefit of the gap analyses and hence could not provide clarity on how the guardrails would fit with other regulation. The Commission sees gap analyses as a prerequisite for designing and introducing AI-specific regulation (including the guardrails).

In some cases, AI-specific legislation may ultimately be required to deal with certain risks of harm or to allow existing legislation to deal with harms (section 'How to identify and respond to legislative gaps'). However, prioritising gap analyses in the first instance is intended to ensure effective regulation (through both existing and new laws) while minimising the potential costs of unnecessary regulation.

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

Regulatory clarity and certainty are important policy tools to support innovation. When firms adopt a new technology, understanding the government's rules of the game, and knowing that changes to those rules are proportionate, risk based, outcomes based and technology neutral where possible (recommendation 1.1), limits the sovereign risks they face. In some cases, regulatory risks will deter adoption of new technology, with negative effects on productivity and international trade competitiveness.

Any new technology-specific regulations will create regulatory uncertainty. New regulations may need to be tested before the courts and could overlap with other existing regulations, either of which would raise regulatory uncertainty. They will also create regulatory costs.

The PC agrees with Westpac's statement that, for example, the 'financial services industry is already subject to extensive regulatory requirements, many of which will apply where AI is used' (2024, p. 4) 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. 3).

The PC understands that regulation cannot and should not be static, and no business has ever faced perfect regulatory clarity. But governments should strive to limit regulatory risk where possible.

As discussed above, the *National AI Plan* expresses a strong preference for relying on existing legal frameworks to mitigate the risk of harm associated with AI use (DISR 2025a, pp. 28–29). This will go some way towards reducing regulatory uncertainty for firms and limit the dampening effect on innovation. As per recommendation 1.2, explicitly committing to the use of technology-specific regulation only as a last resort would add further clarity.

Considering AI-specific regulation once gaps are identified

Once gap analyses of existing regulatory and legal frameworks are completed, and once necessary targeted reforms to those frameworks have been undertaken, it will be clear what remaining harms cannot be mitigated by existing regulatory frameworks and where new technology-neutral regulation is not possible. It is from this basis that the Australian Government should consider the role and design of AI-specific regulation (including the mandatory guardrails).

How to identify and respond to legislative gaps

In its interim report, the PC outlined an approach to responding to the additional risk of harm posed by AI. This involved Australian Governments proactively identifying and acting upon legislative gaps. Generally, the process of proactive gap analysis to regularly review the appropriateness of existing laws is consistent with a regulatory stewardship approach, especially in fast-moving policy areas like AI (PC 2025b). To this end we note that the Australian Government's newly established Artificial Intelligence Safety Institute will 'monitor, test and share information on emerging AI technologies, risks and harms' and will work 'directly with regulators' to safely capture the benefits of AI (DISR 2025b). This will aid the work of regulators and policy agencies undertaking gap analyses.

To aid government agencies in undertaking such gap analyses, the PC has reviewed some of the types of gaps agencies could face and how they could go about responding to them.

The types of gaps in existing legislation that AI could create include:

- **creating new harms** or greatly increasing the risk of previously uncommon harms
- a harm that is covered by existing legislation but **may not apply to AI**
- a harm covered by existing legislation and applies to AI, but **AI use greatly increases risk of harm**
- a harm covered by existing legislation but **establishing liability**, either criminal or civil, could be difficult when AI is used.

Each of these situations is analysed below.

Creating new harms or increasing the risk of previously uncommon harms

If AI has either created a new harm or increased the risk of a harm that was relatively uncommon (and so not previously regulated) then this could create a regulatory gap. New outcomes-based, technology-neutral regulation should be prioritised (possibly through an extension of existing legislation that covers the relevant sector(s)). If technology-neutral regulation is not feasible or is unable to adequately mitigate the risk of harm, then technology-specific regulation could be considered.

An example of this type of gap is distribution of non-consensual 'deepfake' sexual imagery, which was previously difficult and costly to produce. With AI, the creation of such material is very low cost and as a result it has proliferated online. The Australian Government responded to this risk of harm by legislating the *Criminal Code Amendment (Deepfake Sexual Material) Act 2024* (Cth), which made the (non-consensual) distribution of sexual images (fake or real) a criminal offense by amending the Commonwealth Criminal Code. This reform was:

- technologically neutral, in that it applies to non-consensual sharing of sexually explicit material online regardless of whether the material was created or altered using technology (such as AI deepfakes) and
- outcomes based, in that it applied to the harm itself (the distribution of non-consensual sexual images) rather than a particular process (for example, how the AI software itself worked).

A harm that is covered by existing legislation but may not apply to AI

There may be situations where certain acts, if undertaken by a person without the use of AI, are a clear breach of law. However, the legal status of the same act, when undertaken using AI, may be unclear. To remedy this, legislation should make clear that it applies to the use of AI. Examples of this type of gap were found by Treasury (2025c) – in the Australian Consumer Law[8]– and by the TGA (2025a) – in the *Therapeutic Goods Act (1989)* (Cth). These reviews found that some definitions in their legislation had unclear application to AI and recommended that the legislation be amended to clarify its application.

---

[8] Schedule 2 of the *Competition and Consumer Act 2010* (Cth).

For example:

- in the Australian Consumer Law gap analysis it was found that the definition of 'manufacturer' may need to be amended to clarify existing obligations of businesses across the AI supply chain (Treasury 2025c, p. 2)
- in the Therapeutic Goods Act gap analysis it was argued that the definition of several terms including 'manufacturer' and 'sponsor' may need amendment (TGA 2025a, p. 7).

A harm covered by existing legislation and applies to AI, but AI use greatly increases risk of harm

There may be harms that are currently illegal under Australian law, and such regulations apply to AI, but the use of AI makes these harms much more likely. In dealing with this issue, policymakers can either focus on the enforcement of existing laws or greater penalties for breaches of the law. Where these are insufficient to adequately mitigate risk, policymakers could consider technology-specific laws if these would be able to effectively target the harm.

There are several potential risks of harms that AI *may* exacerbate. Participants raised how fraud, privacy and environmental damage – all of which are regulated by existing laws – could be exacerbated by AI (ACCC, sub. 495, p. 14; APDG, qr. 6, p. 5; ATN Universities, qr. 13, p. 3; ASCA, qr. 14, p. 7; Endpoint Strategy, sub. 342, p. 2; OAIC, sub. 356, p. 7; Terri Janke and Company, sub. 164, pp. 6-7). Gap analyses of these issues should analyse whether enhancing enforcement of existing laws (through better resourcing of regulators or greater penalties for breaches of law, regardless of the technology used to harm) is sufficient to adequately mitigate risks. If such steps are not sufficient, then new technology-specific laws could be considered if they are both necessary and desirable. Any new regulations would need to go through the standard cabinet process.

A harm covered by existing legislation but the use of AI makes determining liability, either criminal or civil, more difficult

Some risks of harm are mitigated by holding individuals or corporations legally responsible for any harms that they cause, whether through the civil or criminal justice system. But the use of AI has the potential to make determining and establishing **liability** more complicated. It is beyond the scope of this chapter and this inquiry to comment on all the ways in which the use of AI may complicate how liability is determined. Issues that may need examination include:

- whether, from a policy perspective, it is clear who (as between the AI developer, the deployer, the end user, and so on) should be considered responsible when the use of AI results in harm
- whether, from a legal perspective, the use of AI complicates the process of establishing legal liability– including, for example, whether in given circumstances an AI model might be considered a person's 'agent' or whether the 'black box' nature of AI might mean causation is harder to establish.

Some stakeholders have argued that broad-based, technology-specific regulations such as the previously proposed mandatory guardrails would help resolve some of these liability issues (ADM+S, sub. 412, pp. 9-10).

Generally, the PC considers that the best way to close potential liability gaps will vary according to circumstance and that a one-size-fits-all approach like the proposed mandatory guardrails is too rigid. In some cases the guardrails would not be **necessary** ('high risk' use cases where establishing liability is not an issue) and in other cases they may not be **sufficient**. The guardrails may be a solution for *some* of the diverse liability issues raised by the use of AI under Australian law, but not all. But establishing *which* laws require technology-specific regulation to establish liability is something that should be demonstrated in the first instance through gap analyses (recommendation 1.1).

2. Copyright in the age of AI: finding the right balance

Summary

✱ Australian copyright law requires artificial intelligence (AI) developers to obtain a licence before using copyrighted material to train their models.

✱ However, most AI training occurs overseas where Australian law, including copyright law, does not apply. Some Australian content is being used without permission or compensation in overseas jurisdictions. The legality of this under other countries' laws is uncertain, with litigation ongoing.

✱ Licensing markets are developing for many types of copyright material for AI training. To date, most licensing agreements have been for high-value works with established copyright holders, such as news media corporations and large book publishers. The Australian Government should allow these licensing markets to develop without interference.

✱ But some open web material cannot currently be feasibly licensed, due to very high transaction costs. This content, which is made up of hundreds of millions of active websites, forms the bulk of training material for most large language models and some smaller models.

- Much of this material has been used without permission or compensation for AI training overseas.
- It is unclear whether a licensing market for broader open web material will emerge over time.

✱ Uncertainty in three key areas makes it difficult to design an effective policy response:

- the scope and feasibility of AI-related copyright exceptions overseas
- the effect of AI training on incentives to create new Australian content
- whether licensing markets for open web material will emerge without intervention.

✱ The Australian Government should wait and monitor these uncertainties for three years. If, after three years, the monitoring program shows that these issues have not resolved, the government could establish an independent review of Australian copyright settings and the impact of AI.

- The review's scope could include, but should not be limited to, consideration of whether copyright settings continue to be a barrier to the use of open web material in AI training, and if so whether changes to copyright law could reduce these barriers.
- It could also consider whether copyright continues to be the appropriate vehicle to incentivise the creation of new works and, if not, what alternatives could be pursued.

Creative content – including books, film, song, visual arts and websites – has economic, cultural and social value for Australians. In the words of inquiry participants:

> our art, stories and creative expressions are part of our national identity and must be protected …
> (Airdrie Makim, sub. 576, p. 1)

> cultural and creative activity is recognised as an important part of knowledge-based economies, and makes a valuable contribution to Australia's economic and social wellbeing. (Office for the Arts, sub. 588, p. 2)

Copyright laws restrict the right to copy such works to the creator and anyone to whom the creator grants permission. This allows content creators to profit from their works, and provides an ongoing incentive to produce original content (IP Australia 2025, p. 60). Copyright laws attempt to strike a balance between the social benefits of content creation and the social benefits of freely copying that content in a number of ways, including:

- limiting the length of copyright protection to 70 years after the death of the creator (Horn 2004, pp. 112–113)
- limiting the scope of protection to 'expressions' rather than 'ideas'[9]
- having certain exceptions, such as parody, study and research, that allow copying without the copyright holder's permission (ALRC 2013, p. 49).

AI developers use large datasets containing digital copies of media – such as web pages, books, videos, images and music – to train and refine their AI models to recognise patterns, allowing the models to provide answers to user queries, make predictions and more. These large datasets are required for the proper functioning of the current generation of AI models. While a human can learn from a single example, AI uses 'machine learning' which typically requires a vast number of examples to be able to understand patterns. Participants in this inquiry noted the large and diverse range of materials used.

> Today, billions of webpages fuel AI systems. This has happened quickly at an unprecedented scale. (Creative Commons, Creative Commons Australia, Wikimedia Australia, sub. 250, p. 2)

> AI tools are based on an enormous amount of data copied from the Internet and other repositories … [Data source include] collections of fiction and non-fiction works, films, videos, artworks however it has also included thoughts and opinions from social media and platforms like Reddit. The dark web has also been scraped for its information. (Robert Broad, sub. 190, pp. 7, 9)

This material, which is often protected by copyright, must be copied (at least temporarily) to undertake the training process. Under Australian copyright law, making reproductions of copyright-protected material is the exclusive right of the copyright holder.[10] This means an AI developer must obtain the copyright holder's permission, before making copies. AI developers can do this by obtaining licences (usually for a fee) from the copyright holder.

Most AI training is conducted overseas, by foreign-domiciled companies in foreign data centres. Data on precisely where AI training occurs is scarce, though the vast majority of computing infrastructure used to train AI models is located in the United States of America.[11] Australian copyright law does not apply to AI

---

[9] Copyright only protects the original expression of ideas or information, not the ideas or information themselves. For example, a book that copied the text of a Harry Potter novel would infringe copyright (because the text is an original expression), but a book that merely follows a similar broad plot of a boy finding out he is a wizard and battling an evil wizard, would not (because the broad plot is just an idea).

[10] *Copyright Act 1968* (Cth), ss. 31, 85-88.

[11] As of May 2025, the United States of America is estimated to have just under three quarters of all the world's graphic processing unit performance – a way of assessing capability to train and run AI models, measured here as 16-bit FLOP

training conducted overseas.[12] Instead, any potential copyright infringement is subject to the law of the country where the AI training takes place and any claims must be made through its court system, even if the copyright holder is Australian.

In some overseas jurisdictions, there are copyright exceptions that permit AI training without a licence in certain circumstances. These exceptions may leave some Australian copyright holders without compensation or legal recourse when their works are used without permission. Some AI developers argued that this makes these overseas jurisdictions more attractive locations to train AI models (although the limits of what is permitted is subject to active litigation). For example, the former CEO of Atlassian (an Australian-founded, US-incorporated software company) and current Chair of the Tech Council of Australia, stated:

> Australia has the opportunity to host data centres for the entire Southeast Asia region and potentially beyond … But there are areas which hold us back from an even bigger opportunity …
>
> Australia's copyright laws are out of sync with the rest of the world. Whilst the USA and Europe have fair use or exceptions for text and data mining, and the Australian Law Commission recommended changes in 2014 and the Australian Productivity Commission recommended changes in 2016, we still remain an outlier when it comes to copyright.
>
> This is a barrier to many AI companies training or hosting their models in Australia. This is even a barrier to Australian born companies. (Farquhar 2025)

AI may also reduce content creators' incentives to create new works in other ways, for example by reducing their wages. This may skew the current balance that copyright law tries to strike between providing incentives for creation and public dissemination of that work.

This chapter is a case study in how AI can open gaps in Australia's existing legal framework. It examines whether current copyright laws are a barrier to AI training in Australia, whether copyright law is able to continue to provide effective incentives to creatives with the emergence of AI and what governments should do about this.

In examining these issues, the Productivity Commission is seeking to strike a balance between preserving the incentive to create Australian content against the benefits of enabling AI training. The chapter reflects the information and feedback the PC received in submissions and consultation in response to the information request (on whether reforms to the copyright regime are required to facilitate the development of AI in Australia) in chapter 1 of the interim report.

Australia's copyright settings make domestic AI training less attractive than overseas locations

Most of the economic benefits of AI in Australia will come from using AI models rather than training them. However, attracting domestic AI training would have its own economic benefits, such as greater market investment in supporting infrastructure like data centres. AI models trained in Australia may also be more aligned to Australian experiences and values.

At the moment, Australia's copyright settings make it difficult for AI developers to lawfully access some training material. Other things equal, this encourages AI developers to train their models in other jurisdictions

---

per second (Pilz et al. 2025). China accounts for just under 15%, the European Union just 5% and the rest of the world combined (including Australia) is just under 7%.

[12] For example, s. 36 of the *Copyright Act 1968* says copyright is infringed by a person who is not the copyright owner doing any act comprised in the copyright without license *in Australia*.

where regulatory settings are perceived to present a lower barrier. Reforming copyright settings is one avenue for incentivising domestic AI training, but this would only be justified if it did not greatly reduce the incentive to create new Australian works.

Removing copyright barriers alone may not result in greater AI training in Australia. Other factors affect where AI developers choose to train their models, such as the relative cost of electricity and the availability of skilled labour (Jackson 2025; Thorpe 2025). So, removing copyright-related barriers is potentially a necessary, but not sufficient, condition to attracting AI training to Australia.

No economic modelling exists to understand the likely effect of a change in copyright law on investment in AI training in Australia. Modelling for the United Kingdom estimated that if the country adopted a commercial text and data mining (TDM) exception, investment in 'TDM-related' activities would be £0.8-£1.8bn higher than if they retained the existing non-commercial TDM exception (Europe Economics 2025, p. 1). Given the size of the UK economy, this appears to be a very modest effect.

Is voluntary licensing feasible for domestic AI training?

Some rights holders have begun licensing their work to AI developers, often in exchange for remuneration. If voluntary licensing[13] is likely to develop further and prove sufficient to enable AI training, the Australian Government should wait to see how licensing markets develop before considering other options, such as changes to copyright law. The following discussion considers whether voluntary licensing is likely to emerge for *all* types of training material that AI developers require.

Training AI models requires access to a wide range of content

AI developers need access to a wide variety of materials to train their models (figure 2.1). In Australia, some of these materials are available for use without a licence, such as public domain material ('category 1'), but most are not. Obtaining licences is straightforward in some cases, where the copyright holder can be easily identified and negotiated with ('category 2'). This is the case when dealing with 'traditional' media (such as film, television, journalism, songs and visual art) and larger 'new' media (large online platforms which have the right to and do sublicense their users' content). In other cases ('category 3'), obtaining licences is difficult for individual pieces of content and near impossible for the large amount of this content needed to train many AI models. This is the case for smaller websites and larger web platforms which do not sublicense their users' content.

For AI models that require category 3 materials, the time and cost associated with obtaining these licences will impact the commercial feasibility of training certain AI models in Australia. These costs include not only the licence fees that the AI developers pay to copyright holders, but also the significant transaction costs[14] involved in determining ownership and negotiating bilaterally with (potentially billions of) copyright holders.

---

[13] In this report, 'voluntary licensing' refers to agreements made where a copyright owner willingly grants permission to another party (such as an AI developer) to use their work, often in exchange for remuneration. Voluntary licensing includes direct licensing (where the copyright owner makes an agreement directly with the AI developer) and voluntary collective licensing (where copyright owners authorise a collecting society to negotiate with AI developers on their behalf, and collect and distribute licensing fees to them).

[14] In this context, transaction costs refer to the time and monetary cost of determining ownership of copyrighted material, negotiating with the owner and settling disputes that arise after an agreement has been made.

Figure 2.1 – Copyright status of materials used for AI training

Category 1: free use – license is not required to use for AI training – these include materials in the public domain (for example, where the copyright subsisting in the material has expired) and materials provided under some open use licenses.[a]

Category 2: books, music and films etc – a license is required, and licensing is straightforward – licenses to use these materials for non-AI training purposes are already often sold, whether through direct agreements or collective licenses.[b] Examples include books, academic journal articles, music and film that are distributed by publishing houses or distributors.

Category 3: many websites – a license is required, but licensing is difficult – examples of these materials include lesser-known websites and large websites where the website owner does not have a license to use posted content to train AI models, and ability to sublicense that content to other AI developers. These materials have a vast number of copyright holders, located across the world, and the monetary value of each individual piece of content to the AI developer is low (even if the aggregate training value of the materials is high).

a. For example, much of the material available on the Australian Bureau of Statistics' website is available for use under a Creative Commons BY 4.0 licence (ABS 2025g). Under this licence, the bureau provides broad permission to copy, redistribute, transform and build upon the material for any purpose, even commercially, as long as the bureau is given appropriate credit and the user indicates if changes were made (Creative Commons 2025). **b**. Expanding these licensing arrangements to cover AI training would be easier than for material that has never been subject to licensing.

Voluntary licensing for AI training is emerging for some content

AI developers have begun making agreements with copyright holders to access category 2 materials, such as film, television, journalism, song, visual art and other content posted on some large websites.

Some of these agreements are directly between AI developers and large copyright holders. AI developers tend to seek agreements in two main situations. The first is where the copyright holder has blocked access to its content with paywalls or other technical mechanisms. The second is where the AI developer wants permission for their model to reproduce the training data as verbatim output (which would be illegal without a licence, even under overseas copyright exceptions). The agreements struck between major AI developers and some major media firms, such as OpenAI's agreement with NewsCorp (Smith 2025), fall into this category. Table 2.1 provides some examples of agreements struck for various types of materials.

In many cases, the licensed content has historically been actively managed and licensed by rights holders, such as with books, films and music. But there are also examples of agreements being made for content that has not historically been licensed. For example, Reddit has made agreements with AI developers to provide them with access to content posted on their platform (CBS News 2024). Reddit's terms of service state that users who post content on its platform grant Reddit a broad licence to use and copy that content, including for training AI models, which can be sublicensed (Reddit 2025).

Table 2.1 – AI developers have been making agreements to access some types of training material

Examples of agreements made

Examples of agreements	Type of Material	What the agreements allow[a]
OpenAI & News Corp	News	Train on licensed content and display a subset of licensed content in AI outputs.
OpenAI & Time	Magazines	Train on licensed content and display a subset of licensed content in AI outputs
Elevenlabs & Kobalt and Merlin	Music	Train on licensed content. Agreement requires AI developers to prohibit users from including certain words (such as artists' names, song titles) in prompts.
Unknown AI developer & HarperCollins	Books	Train on licensed content.
Meta & Shutterstock	Images	Train on licensed content.
Microsoft & Informa	Academic journals	Train on licensed content.
Google & Reddit OpenAI & Stack Overflow	Open web content	Access to content to for AI training. Not clear if agreement involves provision of licences under copyright law.

a. Full details of some agreements were not available.

Source: News Corp (2024); OpenAI (2024b); Ingham (2025); Creamer (2024); Shutterstock (2023); Meley (2025); Tong et al (2024); OpenAI (2024a).

Participants in this inquiry emphasised that direct licensing agreements can provide AI developers with efficient and scalable access to content, while contributing to creators' incomes and maintaining their incentives to produce new content. The Australian Publishers Association stated:

> direct agreements between publishers and AI developers are emerging … These mechanisms are tested, flexible, and scalable … when copyright protections are weakened and licensing pathways are undermined, publishers inevitably scale back investment in new local content, leading to fewer titles, reduced diversity, job losses, and a long-term erosion of the cultural and educational resources available to the community. (sub. 523, pp. 1, 5)

Similarly, the Australian Recording Industry Association and Phonographic Performance Company of Australia stated:

> unnecessary downgrades to Australia's copyright laws risk the devaluation of Australia's $8.78 billion music industry … Direct licensing works effectively and efficiently … (sub. 489, p. 3)

Direct agreements can 'allow for greater flexibility in setting terms and conditions for the use of copyright material' (ARIA and PPCA, sub. 489, p. 7). For example, a recent agreement between ElevenLabs (whose AI model generates music from natural language prompts) and Merlin and Kobalt (music rights holders) contains contractual 'safeguards' to protect rights holders. Under these safeguards, ElevenLabs prohibits users from submitting prompts which include artists' names, song or album titles, and substantial or distinct portions of any song's lyrics (Ingham 2025).

There are also examples of collective licensing emerging, such as the Copyright Licensing Agency's upcoming Generative AI Training Licence in the United Kingdom. Collective licences provide smaller copyright holders, who are not in a position to negotiate direct agreements with AI developers, an opportunity

to participate in, and benefit from, AI training (Cormack 2025). Collective licences also provide AI developers with access to a large amount of content at a lower transaction cost (though not necessarily lower licensing costs), as developers negotiate with the collecting society, rather than the many individual copyright holders.

No changes to Australian law are required to facilitate the voluntary licensing of category 2 materials, which should be allowed to continue to develop. Direct and collective licensing of these materials is relatively efficient, providing AI developers with access to large amounts of content at relatively low transaction costs (since the rights holders typically hold rights to large amounts of content and are easy to identify). Such licensing also creates more incentives for the production of new creative content, to the benefit of both the public and AI developers. However, some participants in this inquiry argued that transparency obligations should be introduced to strengthen licensing markets (box 2.1).

Box 2.1 – Are transparency obligations required to support licensing markets?

Several participants in this inquiry recommended introducing transparency obligations that would require AI developers to disclose the materials they have used to train their models (ARIA and PPCA, sub. 489, p. 9; Australian Society of Authors, sub. 478, p. 19; Penguin Random House Australia, sub. 477, p. 3). Some argued that, without this transparency, copyright holders are unable to determine if AI developers have used their content without permission. This makes it difficult for the holders to enforce their rights, which in turn undermines licensing markets.

A counter view is that a model's training dataset is a core part of what sets it apart from competitors' models, and that disclosure would allow competitors to replicate the original AI developer's dataset and compromise its competitive advantage. In relation to a proposed bill that would introduce transparency requirements, the California Chamber of Commerce said:

> … data and datasets is part of what differentiates [AI] providers, thereby causing significant concern among developers as to the potential of this bill to undermine their intellectual property and harm competition. (2024, p. 1)

Requiring dataset transparency could discourage AI developers from investing as much in curating high quality training datasets and have a chilling effect on innovation.

Some jurisdictions have implemented forms of transparency requirements. For example, the EU's *Artificial Intelligence Act 2024* requires providers of general-purpose AI models to provide 'a sufficiently detailed summary about the content used for training of the general-purpose AI model, according to a template provided by the AI Office' (art. 53(1)(d)). The template is meant to strike a balance between the interests of copyright holders and the need to protect trade secrets,[a] but a coalition of 40 EU rights holder organisations criticised it for failing to deliver sufficient transparency (European Writers' Council 2025).

a. Explanatory Notice and Template for the Public Summary of Training Content for general-purpose AI models required by Article 53(1)(d) of Regulation (EU) 2024/1689, p. 5.

Voluntary licensing may not allow access to some open web material

While pathways are developing for access to category 2 materials, it is unclear whether voluntary licensing solutions will develop for access to most category 3 materials. This includes smaller websites and larger web platforms which do not sublicense copyright-protected content posted by their users. At this point in time, the only large web platforms the PC is aware of that have made agreements with AI developers for access to

content posted by their users are Reddit (a news and discussion website) and Stack Exchange (a question and answer website) (CBS News 2024; Wiggers 2024). Some large platforms, such as X (a social media platform), have the right to sublicense their users' content to third parties, but have not done so yet (X 2024). Others, such as Youtube, are leaving it to their individual users to decide whether to allow third-party AI developers to train on their content (Youtube 2024).

As noted above, the copyright in most category 3 content is owned by a large number of individual copyright holders – by some estimates, there are over 200 million active websites online (Reboot Online 2025) and some large web platforms have *billions* of users. Furthermore, these copyright holders are often hard to identify. A lot of online content lacks any information that would help to identify the rights holder (Meta Platforms 2023a, p. 20), and in jurisdictions like Australia and the United States, copyright vests automatically in the content's creator so no database of copyright owners exists.[15]

At present, the transaction costs to identify and negotiate with such a large number of hard-to-find rights holders make direct licensing of category 3 material commercially infeasible (Meta Platforms 2023a, p. 17). The US Copyright Office also concluded that licensing of some copyrighted content (such as blogs and internet reviews) would be difficult in its third report on *Copyright and Artificial Intelligence*.

> There are copyright sectors where licensing infrastructure does not yet exist and may be difficult to build … Administrative or transactional costs can pose particular challenges when works are created outside of professional creative industries or are not intended to be monetized, or when ownership is diffuse. Transaction costs in some cases might exceed the value of the works for training and render direct licensing infeasible. (2025a, pp. 70–71)

It is also unclear whether these copyright holders would opt in to any collective licensing agreements. The value of any single, less popular website to an AI model is very low as the removal of a single site would have almost no effect on the quality of the model. Because of this, the compensation AI firms would be willing to provide to smaller websites is likely very low. So even if the copyright holders are not opposed to their material being used to train AI, the low remuneration they would likely receive may provide inadequate incentive to engage with a collecting society. If AI developers continue to face difficulties in obtaining licences to train on open web material, they are unlikely to train their models in Australia.[16]

There are some emerging developments which may make the voluntary licensing of category 3 materials more feasible over time.

First, more large websites may change their terms of service to provide themselves with broad licences to use content posted on their platforms for training AI models (and the ability to sublicense to other AI developers). This could unlock voluntary licensing for a lot of open web content that would otherwise be commercially infeasible to access.

Second, technical solutions are being developed to automate licensing, which may reduce the transaction costs of negotiating direct agreements. For example, organisations like Cloudflare (a network security and web infrastructure company) are developing tools to allow copyright holders to restrict AI crawlers' access to their websites and set per-crawl prices for a licence to scrape their content (Allen and Newton 2025).[17] This

---

[15] The United States of America does have a copyright database, but registration is not required to obtain copyright protection. Registration on the database does provide some legal enforcement benefits, but copyright holders of open web content (like blogs and lesser-known websites) are unlikely to register, as few seek to commercialise their content and so do not need to enforce their copyright.

[16] Training in Australia on these open materials without a licence would infringe copyright.

[17] 'Crawling' and 'scraping' websites refers to the use of software to automatically visit websites, read their pages, and collect information from them. Crawlers copy text, images and other content and store that data in large databases.

means that the AI developer would not have to incur search costs in trying to identify the copyright holder, or even directly contact them to negotiate agreements. However, it is unclear how effective these technical solutions will be at blocking AI crawlers from scraping without permission, and whether AI developers and copyright holders will be able to find mutually acceptable prices for these licences, when the value of each individual piece of content is very small.

Third, as case law develops, it will become clearer whether scraping online content is permitted under overseas copyright regimes. If, for example, US courts decide that the fair use exception does not permit training on scraped open web content, AI developers may have to obtain licences to train using this material in the United States. This would make Australia relatively more attractive as an AI training destination, as AI developers would have to negotiate with smaller copyright holders regardless of whether they train in Australia or the United States.[18]

Difficulty licensing open web material would likely constrain Australian AI development

General-purpose generative AI models (the multimodal LLMs or chatbots that many are now familiar with) require large amounts of open web data for training. A prominent free repository of web crawl data called Common Crawl provides an 'estimated 70-90% of the tokens used in training data'[19] for many LLMs (Common Crawl 2025). Common crawl likely contains predominately open web, or 'category 3' data (although no precise estimates are available). Indeed, Meta stated that the high-performing LLMs of today were trained on datasets containing 'billions of pieces of text from millions of individual websites' (Meta Platforms 2023a, p. 20).

The commercial infeasibility of using some open web data constrains the functionality of any general-purpose models trained in Australia, making it a less attractive location for training these models.

Some small, specialist AI models also need access to open web data for training. For example, an image recognition AI model may benefit from training on material posted by individual users online.

An AI system trained on licensed stock photographs, for example, may be capable of identifying an elephant in a National Geographic spread, but might be incapable of finding an elephant in a cartoon meme or a child's drawing because it lacks a complete model of the concept of an 'elephant'. (Meta Platforms 2023b, p. 4)

The lack of access to open web data also affects non-commercial uses of AI. For example, a scientific research organisation may want to develop an AI model to analyse political sentiment or views on the social acceptability of a new technology. Such a model would need to be trained on open web material, where such sentiment is often expressed.

If pathways for AI developers to access open web material fail to emerge, the amount of AI training that occurs in Australia will continue to be constrained. Indeed, even if licensing markets for open web material

---

These databases can then be used for various purposes such as training AI models or helping search engines (like Google Search) retrieve information for users.

[18] The US Copyright Office (2025a, p. 71) noted that the inability to obtain a license would, all else equal, make a finding of fair use more likely as this means the use does not deprive the copyright holder of licensing income. That said, for some open web materials, other factors may outweigh the absence of licensing markets depending upon how the material is used in the model.

[19] As defined by NVIDIA (2025), tokens are 'units of data processed by AI models during training and inference, enabling prediction, generation and reasoning'. They can be thought of as representing the information contained in a text, video, image or audio file. More tokens mean more information.

do emerge, AI training in Australia may still lag due to the option of training AI models in overseas jurisdictions that allow free access to certain copyrighted materials.

The challenges of designing a policy response

While copyright law may currently constrain AI training in Australia, the design of effective policy to address the issue is hindered by uncertainty in three key areas.

- The scope and feasibility of AI-related copyright exceptions overseas – which make the relative attractiveness of Australian AI training unclear under status quo copyright settings.
- The effect of AI training on incentives to create Australian content – which means that the effect of any changes to copyright law would have uncertain effects on existing Australian economic activity.
- Whether licensing markets for open web material would emerge without intervention – which means that it is unclear whether changes to copyright settings are needed to attract domestic AI training investment.

The PC considers that these **three uncertainties** – discussed in more detail below – are potentially barriers to any policy change.

The scope and feasibility of AI-related copyright exceptions overseas

Several countries – including the United States and the countries in the European Union – set limits on their AI-training related copyright exceptions, including through 'fair use' requirements and opt-out provisions. These limits may mitigate the negative effect on incentives to create new content caused by copyright exceptions. However, in many cases, the boundary between allowable and non-allowable uses remains uncertain or difficult to enforce. Until these legal uncertainties are resolved, it is unclear to what extent Australia's copyright settings present a barrier to domestic AI training.

The United States: defining the boundaries of fair use

Under the United States doctrine of fair use, legislation identifies factors to be considered in determining if a use is fair (Copyright Act 1976 (US), §. 107). These factors include the 'effect of the use on the potential market' for the work and the 'purpose and character of the use,' including how transformative the use is. However, it is the courts that determine how these factors should be weighed in each case.

AI technology is relatively new, so the relevant case law is still developing. As at May 2025, there were over 40 ongoing cases against AI developers (Levi and Ghaemmaghami 2025). But few cases have been heard in appellate courts whose decisions would provide authoritative legal precedent that binds lower courts, and none by the Supreme Court, leaving the boundaries of 'fair use' uncertain.[20] It will likely take several years for this case law to develop. Given that the vast majority of AI infrastructure is in the United States (footnote 3), policymakers should monitor how the AI-related boundaries of fair use develop.

How US courts draw these boundaries will influence Australia's *relative* attractiveness as a location for AI training. If US courts interpret exceptions narrowly – requiring licences in many cases, as under current Australian law – Australia's copyright system may become relatively more appealing than it is now and

---

[20] In the United States of America, appellate courts are the first point at which a jurisdiction can obtain binding precedent – rulings that must be followed by lower courts within that jurisdiction (Legal Information Institute 2025). Decisions from trial courts (lower in the hierarchy than appellate courts) may be persuasive but are not binding. The Supreme Court's decisions are binding on all other courts in the country, as it is the highest court.

changes may not be necessary to attract domestic AI training. Conversely, if overseas courts interpret copyright exceptions broadly, Australia may attract limited AI-related investment under its current settings.

The European Union: still trying to make an opt-out work

In the European Union, legal uncertainty comes not from a lack of case law but from unclear rules on how the 'opt-out' provisions in their TDM exception work. Two TDM exceptions are embedded in the EU Digital Single Market Directive (EU 2019/790) – one for scientific research (article 3) and another for general use (article 4). The general use exception allows the use of copyrighted works for TDM, including for commercial purposes, provided that the rights holder has not reserved their rights (that is, opted out). This model was intended to encourage innovation and provide more legal certainty for TDM activities, while also providing rights holders with an opportunity to opt out and license their works to organisations undertaking commercial TDM (Ziaja 2024, p. 454).

However, the opt-out mechanism has resulted in uncertainty for both rights holders and AI developers. The directive does not specify a standardised way of opting out, resulting in rights holders attempting to opt out in a wide variety of ways (Lucchi 2025, p. 55). This has made it difficult for AI developers to determine whether a legally effective opt-out has been made for a work (Bersh 2024, p. 352), seemingly undermining the legal certainty that the TDM exception was intended to provide. Indeed, the European Union's Policy Department stated that the exception 'neither reliably permits nor clearly prohibits AI training – leaving all stakeholders in a regulatory limbo' (Lucchi 2025, p. 56). The European Commission is exploring the feasibility of a central opt-out registry (European Commission 2025), but this has not yet been implemented. So far, the European Union is the only jurisdiction to attempt to implement an opt-out provision for a text and data mining exception, though the United Kingdom has been considering a similar provision (UK Government 2024a).

Until the European Union clarifies how its opt-out mechanism works, the limits of AI training there will be uncertain. This could have two potential outcomes. If rights holders are unsure how to opt out, developers may be able to train on copyright materials effectively without limits. This would make the EU more attractive as a place to train AI and Australia relatively less attractive under current copyright settings. Alternatively, if developers fear that rights holders have opted out but cannot be certain, they may avoid training AI in the EU to reduce legal risk. This would make Australia more appealing as an AI training location under status quo copyright settings.

Almost all TDM exceptions were not intended to allow AI training

It should also be noted that, as far as the PC is aware, no countries introduced their copyright exceptions for the purpose of facilitating AI training except for Singapore (Singapore Ministry of Law 2021, para. 55). Most of these exceptions predate the significant rise in public awareness of AI that followed the release of ChatGPT in late 2022 (figure 2.2). Since 2022, no country has introduced copyright exceptions for AI training or TDM, and some policymakers in those jurisdictions have expressed concern that their existing TDM exceptions allow uncompensated use of copyrighted material for AI training.

Figure 2.2 – Timeline of overseas copyright exceptions

2019: the European Union introduced its TDM exceptions and Japan's exception for non-enjoyment uses came into force

2007: Israel enacted its fair use exception

Late 2022: initial release of ChatGPT

1976: the United States codified its fair use exception

2014: the United Kingdom enacted a TDM exception for non-commercial research

2021: Singapore introduced its computational data analysis exception

Sources: Chow (2024), Elkin-Koren and Netanel (2021, p. 1122), Frosio (2020), Hays (2024), Marr (2023), UK Intellectual Property Office (2014), US Copyright Office (2025b).

The UK Government launched a consultation process in December 2024 on a proposed EU-style TDM exception, which would cover commercial TDM but be subject to opt-outs (UK Government 2024b). The results of this consultation have not yet been released. However, the proposal has faced significant opposition from the creative sector, who raised concerns that an opt-out system may fail to adequately protect copyright holders and that the exception may undercut emerging licensing markets (ALCS 2025, p. 3; Booth 2024). This has left the future of the reforms in a state of flux.

There have been calls for existing exceptions to be reformed. A report commissioned by the European Parliament's Policy Department for Justice, Civil Liberties and Institutional Affairs[21] concluded that the European Union's TDM exceptions 'were not designed for large-scale model training', and that training AI models on protected works without compensation 'undermines the economic rights of creators and threatens to erode the copyright system's foundational incentive structure' (Lucchi 2025, pp. 12, 49–50). It goes on to recommend that the European Union 'clarify legislatively that Article 4 was never intended to, and does not, extend to generative-AI training' and restore an opt-in system (which would require licensing for all content prior to its use for AI training) (2025, p. 122).

The effect of AI training on incentives to create Australian content

AI could affect the incomes of content creators in several ways – some positive and some negative.

On the positive side, AI is expected to boost overall productivity, which could lift average incomes and increase demand for creative content, whether made by people or by AI. AI can also help creators work more efficiently by supporting or automating parts of the creative process, which may raise their incomes.

---

[21] This department provides in-house and external expertise to support European Parliament committees and other parliamentary bodies in shaping legislation (Lucchi 2025, p. 2).

Furthermore, as discussed above, some AI companies are now paying for access to human-created content to train their models.

On the other hand, AI-generated content can also compete with human-made work, potentially lowering demand for some types of human-created content and hence reducing creator incomes.

Overall, it is still uncertain whether AI will increase or reduce creator incomes. Some peak creative sector bodies have commissioned modelling that forecasts creator income losses (APRA AMCOS 2024, p. 10; CISAC 2024, pp. 67, 83). However, as with any projection of the future, there is a high degree of uncertainty surrounding these figures. The possible effect of AI on creators' incomes is discussed in more detail in appendix D.

If the income creators receive from producing new content falls, the economic incentive to create that work will fall too. This could have a negative effect on productivity. AI models require new, human-made content to train on – if less new human-made content is produced, the speed at which AI models improve could slow (Getty Images, sub. 262, p. 3; Sony Music Australia, sub. 429, p. 5), decreasing the productivity growth from AI's adoption and use.

If, over the next several years, the uncompensated use of copyrighted material for AI training significantly reduces Australian creators' incomes, policymakers could consider compensated mechanisms – such as statutory or collective licensing schemes – that permit AI training while supporting creators. If creators' incomes continue to grow, and the uncertainty about limits on AI training resolve, introducing AI-related exceptions – such as those discussed above – may be appropriate.

Whether licensing markets for open web material will emerge without intervention

Reforming copyright law to allow AI training on open web material is only desirable if licensing markets would not emerge without intervention. Poorly implemented intervention could distort or prevent their development.

Several factors will likely shape whether licensing for open web material emerges in the coming years. As discussed above, one is how broadly overseas courts interpret AI-related copyright exceptions – the broader the interpretation, the weaker the incentive for AI developers to seek licences. Another factor is whether technological solutions, such as those being implemented by internet security companies like Cloudflare, can effectively prevent unauthorised uses of open web content. If these tools succeed, licensing markets become more likely.

The Australian Government must consider these three uncertainties in deciding how to get the copyright balance right.

Getting the copyright balance right

As previously discussed, copyright aims to balance incentives for creators to produce new works against the public benefits from accessing and using those works. The emergence of AI has seemingly disrupted that balance in the short term.

A range of options could be considered to reestablish that balance. Three options – some of which we asked for submissions on in our interim report (1-2) and one of which is being discussed by the Australian Government's Copyright and AI Reference Group (CAIRG)[22] (2) – are discussed and evaluated below:

1. a fair dealing text and data mining exception
2. extended collective licensing
3. wait to see if voluntary licensing markets develop.

A fair dealing text and data mining exception

A fair dealing exception for TDM would allow AI developers to use copyright material without permission from the copyright owner to train their AI models, as long their use is '**fair**' in the circumstances.

The fairness requirement could require courts to consider the effect of the use on the market for, or value of, the work. This could leave space for voluntary licensing to co-exist with the exception, for uses which are not deemed fair.

The introduction of a fair dealing exception for AI training could result in legal uncertainty until case law is developed through litigation. To reduce this uncertainty, and rather than just waiting for precedent to develop, any proposal for a TDM could consider the use of legislative criteria or regulatory guidance to provide clarity on what uses are likely to be considered fair.

The PC's interim report included a request for further information on the desirability of having a TDM. In response, the PC received hundreds of submissions focused on the pros and cons of a TDM exception. This feedback has been very important for helping the PC form its final view. Box 2.2 captures at a high level some of the main points raised. The range of views expressed in submissions, including on a TDM exception, are also further discussed in the accompanying 'What We Heard' paper.

Overall, while some submissions, including those from technology companies and some research institutions, expressed support for a TDM exception, content creators and collecting societies were concerned about the potential for erosion of content creator incomes.

An exception for non-commercial TDM

A copyright exception for non-commercial TDM would allow the use of copyrighted materials for TDM (including AI training) without permission for strictly non-commercial activities only. It could facilitate greater development and use of AI in fields such as scientific research and education. CSIRO highlighted that for Australia to:

> stay at the forefront of AI understanding, research and development … Australian research organisations [must] have the necessary freedom to undertake scientific research without inappropriate exposure to copyright infringement liability. (sub. 322, p. 2)

In the education context, the Copyright Advisory Group – Schools (CAG Schools) said that a non-commercial AI training exception would permit the 'development of local, education-specific AI tools and AI-enabled technologies', which are critical for 'Australia's vision for a modern education system' (sub. 517, p. 22).

---

[22] CAIRG is a working group of creatives, collecting agencies and technology firms, established by the Attorney General's Department to engage with stakeholders on 'copyright challenges emerging from AI' (Dreyfus 2023).

Box 2.2 – Views on the desirability of a text and data mining exception

Many rights holder organisations argued that a TDM exception is not necessary to facilitate AI training in Australia, and that licensing markets under current copyright settings can readily provide AI developers with access to training materials. For example, the Copyright Agency said:

> it is not necessary to introduce a text and data mining (TDM) exception to facilitate AI development in Australia … [Australia's Copyright Act] is sufficiently technology-neutral and flexible to enable the continued development of content licensing arrangements to support Australian AI development. (sub. 473, p. 1)

Many submissions expressed concern about the effect of a TDM exception on the incomes of creatives and the associated effect on the incentive to create and contribute to Australian culture. For example, the Australian Publishers Association said:

> [a TDM exception] would undermine Australia's copyright framework and expose the sector (and the nation) to significant cultural and economic harm … By making large-scale copying free, these exceptions would undermine the business case for publishers and information providers who invest heavily in producing, organising, and maintaining high-quality datasets. (sub. 523, pp. 3–4)

Several organisations from or representing the tech industry advocated in favour of a text and data mining exception, arguing that it would provide AI developers with the legal certainty they need to train AI models in Australia and pointing out the benefits that this may have for the Australian economy. For example, Microsoft said:

> Microsoft supports … introducing clear Text and Data Mining (TDM) exceptions to enable data analysis of publicly available data including AI and machine learning developments while, at the same time, continuing to protect expressive works … [A recent UK study] found a commercial TDM exception to have broader impacts on increasing investment in other sectors including scientific and academic research, legal and financial analysis, and healthcare and pharmaceuticals. (sub. 574, p. 4)

The Copyright Act already contains a fair dealing exception for research and study and a statutory licence for education institutions. However, CSIRO argued that uncertainty about how the fair dealing factors would be applied by courts in the context of AI research projects means that 'there are significant impediments under the current law to confidently rely on the research/study fair dealing exception' (sub. 322, pp. 2–4). And while the statutory licence may already allow education institutions to use copyright materials to train AI models, CAG Schools argued that its scope is overly broad, requiring payment for all forms of online content, even where the content has 'no commercial value' and where the copyright holder has 'no expectation of payment' (CAG Schools, sub. 517, p. 21). As such, CAG Schools and CSIRO advocated for the introduction of a non-commercial exception (CAG Schools, sub. 517, p. 4; CSIRO, sub. 322, p. 4).

Any proposal for a non-commercial TDM would have to consider:

- whether it is possible to distinguish between commercial and non-commercial AI training, which some participants in this inquiry have argued would be complicated because outputs from scientific research may have commercial applications (Arts Law, sub. 490, p. 12; Wiley, sub. 756, p. 3)

- whether the exception should be subject to a fairness test, or whether the non-commercial purpose of the AI training is sufficient to protect the interests of copyright holders
- whether amending or clarifying the existing fair dealing exception for research and study, rather than creating a new exception, would be sufficient.

It is too soon for a TDM exception

Introducing a TDM exception before the three uncertainties (discussed above) are resolved risks distorting – or even preventing – the development of licensing markets for AI training. A TDM exception could weaken incentives to produce Australian creative content. And if overseas courts interpret the scope of their copyright exceptions narrowly (requiring licensing in most cases), then Australia's current settings may become relatively competitive. This is because regardless of whether developers train AI models in Australia or overseas, a licence will likely be required for access to copyrighted content.

Policymakers could attempt to limit distortions by confining a TDM exception to open web material, but this may not be workable. 'Open web' is merely a mode of publication; the same piece of creative work might appear both online and in print (such as some newspapers and magazines). A TDM exception for open web material would likely also capture some category 2 material published in multiple formats, interfering with those licensing markets. Moreover, Australian and international law do not provide a clear legal distinction between open web content and other types of material that could easily be adopted.

Another option is an opt-out mechanism. However, as explained above, only the European Union has implemented an opt-out as part of a TDM exception and this has not to date been successful. Australia would have limited international precedent on which to base the design of such a system.

If a TDM exception was adopted and then later found to harm creative incentives or have other unintended effects, repealing its effects would be difficult. Once AI developers train models using copyrighted material under the exception, those models retain this knowledge as long as the model continues to be used. If these models reduce the incentives to create new content, repealing the exception may not reverse the resulting harms.

We note that the Australian Government has explicitly ruled out a TDM exception (Rowland 2025). Instead, it has committed to consulting with the CAIRG on options to 'encourage fair, legal avenues for using copyright material in AI' including paid collective licensing agreements or maintaining the status quo.

However, most of the current problems with implementing a TDM exception may diminish over time. If US courts interpret fair use broadly, an Australian TDM may be more effective in attracting AI training investment. If open web licensing markets fail to develop, then an Australian TDM exception is unlikely to be distortionary. And if AI is shown to have only minimal effects on creative incentives then the potential costs of a TDM exception also decline.

Extended collective licensing

Under extended collective licensing (ECL), the Copyright Act would authorise a collecting society to manage the licensing of copyrighted works (including that of the collecting society's members and non-members) unless the rights holder opts out. The nominated collecting society would negotiate rates and terms with AI developers and collect and distribute fees to participating copyright holders.

An ECL scheme would allow AI developers to negotiate with a single collecting society for access to a large amount of content, helping to reduce the transaction costs associated with licensing open web material. And the opt-out mechanism could, if implemented well, allow rights holders of category 2 materials (like books, music and film) to reserve their rights and negotiate direct agreements with AI developers, helping to preserve emerging direct licensing markets.

Extended collective licensing may not attract investment and is logistically difficult

However, implementing an efficient opt-out mechanism may be difficult. As discussed above, the European Union has had difficulties with finding an efficient, standardised opt-out mechanism, leaving rights holders unsure if they have effectively opted out, and AI developers unsure of whether they can use any given piece of content to train their models.

An ECL also has the potential to distort creative incentives if the extended licence provides too little compensation to copyright holders.

Furthermore, an ECL scheme may fail to attract more AI training if overseas exceptions are interpreted broadly. If overseas exceptions are interpreted broadly, AI developers may still prefer to train their models overseas where they can use copyrighted content for free, rather than training their models in Australia where they would have to pay fees to obtain a licence under the ECL scheme.

ECL also faces logistical challenges. The body administering the scheme would need to keep records of up to hundreds of millions of websites as well as hold details about their rights holders. It would then need to collect payments from AI companies based on what material they used and apportion this compensation among the millions of rights holders.

As noted above, the Australian Government is currently consulting with the CAIRG on whether to adopt an ECL scheme (or a compulsory statutory licence, without an option to opt out) and how to design such a scheme. This process would need to overcome the implementation obstacles noted above and would still be subject to the uncertainties surrounding the boundaries of overseas copyright exceptions.

Wait and monitor the situation

Under this option the Australian Government would wait for several years to see how the three uncertainties play out before taking any policy action. During those years, the government would gather information necessary to monitor developments in Australia and overseas with respect to copyright settings, licensing markets and creative incomes.

This is the productivity maximising option. All other options would involve making policy decisions without adequate information which could result in poorly implemented solutions or distorted licensing markets.

Depending on how these issues evolve, the Australian Government should consider a broader review of copyright settings and the impact of AI as well as the suitability of the copyright system as an appropriate vehicle to encourage creation of new works.

This approach aligns with recommendation 1.2 of this report, that AI-specific regulation should only be considered as a last resort when it is not feasible to adapt existing legal frameworks.

» **Recommendation 2.1**
A review of Australian copyright settings and the impact of AI

The Australian Government should monitor the development of AI and its interaction with copyright holders over the next three years. It should monitor the following areas:

- licensing markets for open web materials
- the effect of AI on creative incomes generated by copyright royalties
- how overseas courts set limits to AI-related copyright exceptions, especially fair use.

If after three years the monitoring program shows that these issues have not resolved, the Australian Government could establish an independent review of Australian copyright settings and the impact of AI. The review's scope could include, but not be limited to, consideration of whether:

- copyright settings continue to be a barrier to the use of open material in AI training, and if so whether changes to copyright law could reduce these barriers
- copyright continues to be the appropriate vehicle to incentivise creation of new works and if not, what alternatives could be pursued.

3. Rightsizing data access

Summary

✳ **When individuals and businesses can easily access and share data that relates to them, they can get more value from the products and services they use and try new ones. They can also access useful insights and advice to make better decisions. These benefits can boost innovation and competition, potentially creating productivity benefits worth up to $10 billion a year to gross domestic product.**

✳ **The Australian Government has implemented some significant policies to improve data access, including the Consumer Data Right (CDR).**

- The CDR has made strong progress in banking and energy after a slow start. The CDR is designed as an economy-wide framework, but its accreditation model, bespoke privacy safeguards and technical requirements are too onerous for most sectors.

✳ **Data access for consumers is inconsistent across the economy, but data markets are quickly evolving.**

- In many cases, such as in the retail and agriculture sectors, data access solutions are emerging in response to competition and consumer demand. These solutions allow consumers to bring together non-standardised or unstructured data that is available from the products and platforms they use.
- The development of artificial intelligence and related technologies may reduce the access costs for consumers over time and enable them to consolidate information more easily.

✳ **The Australian Government should commit to reforms that will enable the CDR to better support data access for high-value use cases where data markets fail to evolve, while minimising compliance costs so it can bring better value to consumers and businesses into the future.**

- In the short term, the government should enable consumers to share data with third parties and simplify the on-boarding process for businesses. It should also commit to aligning the CDR's privacy safeguards with the Privacy Act (chapter 4) and enabling access to selected government-held datasets.
- In the long term, the CDR framework should be significantly amended so that it has the flexibility to support a broader range of use cases where the CDR is required, by making the accreditation model, technical standards and designation process less onerous.

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 past few decades and new technologies – such as artificial intelligence (AI) – unlock new uses and value-adding opportunities for this data (figure 3.1).

Figure 3.1 – Data created over time
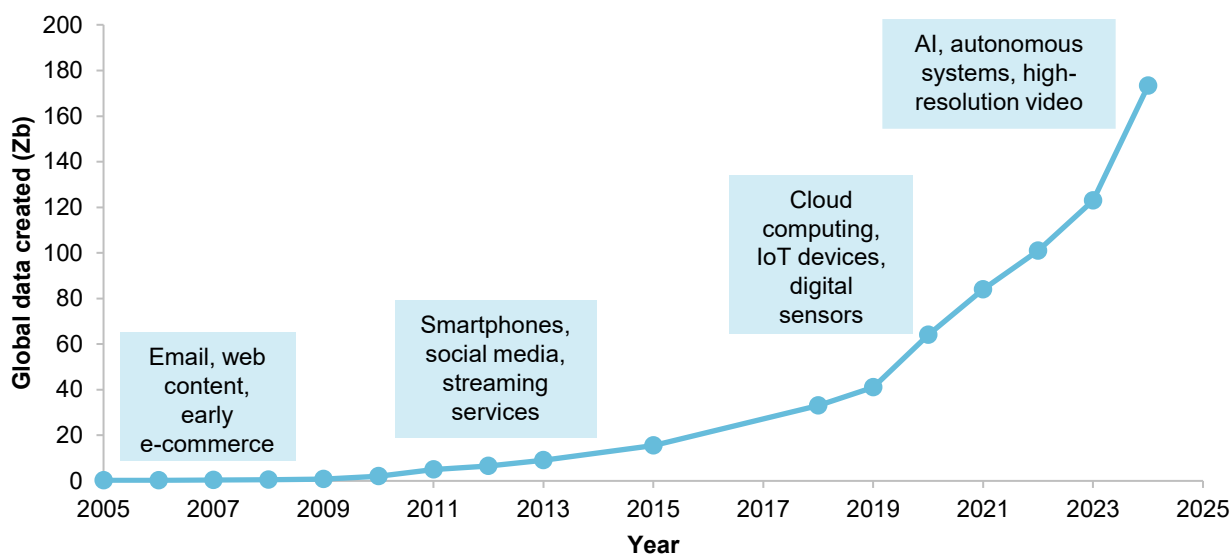
Source: Dell (2009); Gantz (2008); Gantz and Reinsel (2012); Hilbert and López (2011); Reinsel (2007); Taylor (2025); Tweney (2018).

This data is monetised, traded and shared with other parties (Fernandez et al. 2020, p. 11). But it takes considerably more effort for you, the data subject, to access and share that same data about yourself. For example, consumers might need to resort to unofficial third-party tools to access and share data, which can have security and potentially warranty implications.

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 is only accessible in a way that limits its use.

The Australian Government administers several initiatives aimed at improving the state of data access and sharing in Australia. The most ambitious of those is the Consumer Data Right (CDR). The CDR was designed with the capability to operate across the whole economy, but currently only operates in the banking and energy sectors (Australian Government 2024). It allows customers to authorise data holders to share fine-grained transaction data with Accredited Data Recipients via secure, standardised Application Programming Interfaces (APIs) (Australian Government 2024, 2025e; Jones 2025).[23] This functionality is used by a suite of apps that assist consumers with personalised budgeting (for example, Frollo), accessing financial services (for instance, WeMoney) and improving their household energy efficiency (such as EnergyFlex) (Open Finance ANZ 2025, p. 18).

The CDR is by design, a heavily-regulated, highly-secure data-sharing platform (Australian Government 2024; Treasury 2023a, pp. 7–8). To participate, businesses need a relatively high level of data sophistication and maturity, and meeting this bar can require significant expenditure (Treasury 2023a, pp. 11–13).

But the CDR is 'too much' for some sectors. Some sectors do not have the data maturity to implement it. In other sectors, the typical use cases for data do not require the security, sophistication or continuous/high-frequency data access the CDR provides. Recognising this, the Productivity Commission's

---

[23] The CDR was established under Part IVD of the *Competition and Consumer Act 2010* (Cth) and first introduced in 2019. It gives the responsible Minister powers to designate sectors by specifying the data holders who must participate, and the classes of data they need to share (Treasury 2022b, p. 86).

Harnessing Data and Digital Technology interim report raised the idea of the Australian Government creating lighter-touch 'data pathways' that would operate separately to the CDR.

However, when we consulted with industry participants and looked at two case studies in more detail – one in the retail sector and one in the farm sector – we found evolving, and in many ways, sophisticated and competitive data sharing environments. We did not identify a clear gap for government intervention over and above existing regulations that implicitly or explicitly regulate data sharing (these include, at present, the CDR and the Privacy Act).[24]

While these data markets are not perfect, the trade-offs for consumers – in terms of time spent, for example, downloading individual digital receipts or doing manual data entry – are not insurmountable. Moreover, additional government intervention could just as likely hinder these evolving markets (for example by imposing standards and rules) as it is to speed their development. These markets often are dealing with data that is relatively non-sensitive and hence the downside cybersecurity risks associated with unofficial data access tools like screen scraping – which can allow consumers to automatically aggregate data from multiple digital accounts – are less of a concern.

As such, the priorities for the Australian Government, in terms of expanding data access and sharing, should be twofold.

1. Optimise existing data sharing initiatives, with the immediate goal of making the CDR work better for businesses and consumers in the banking and energy sectors (where it already operates). This means facilitating data sharing with third parties, providing a simpler on-boarding process for businesses, and enabling access to selected government-held datasets.
2. In the long term, make the CDR a more flexible data access and sharing platform to support a broader range of use cases. This would involve making the accreditation process and technical standards less onerous.

While data access and sharing initiatives for banking, health and energy data are delivering value in Australia, these initiatives can do much more (box 3.1) (Jones 2024b; PC 2024a, p. 15). Productivity gains from greater data sharing could create benefits to GDP worth between $1 billion and $10 billion (appendix B). To help realise these gains, a reformed CDR must be easier and cheaper to access for businesses and consumers. The government has enunciated a reform agenda to this end, and we support that agenda being advanced with urgency (Jones 2025). To be clear, not every data use case should be subsumed into, or regulated by, the CDR. In many cases, private market data access solutions like the ones we analysed in this inquiry will emerge in response to competition and consumer demand. The CDR should ideally be considered where there are structural or technological constraints that are clearly hindering the development of consumer data access.

---

[24] The *Privacy Act 1988* (Cth) sets out how regulated entities must handle personal information. It includes 13 Australian Privacy Principles (APPs), including APP 12, which specifically requires certain entities that hold personal information to give individuals access to the information (subject to limited exceptions) within a reasonable timeframe and, where practical, within the requested form (OAIC 2019, 2023d). Further discussion of the Privacy Act can be found in chapter 4 and appendix F.

Box 3.1 – **How do people and businesses benefit from data access**

Better data access will benefit people and businesses and promote competition and innovation across the economy. 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 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 2024, pp. 83–88).

Data access unlocks an analogous set of benefits for businesses. Firms can use data to identify business process improvements, unlock additional 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 candidates and by expanding credit access for borrowers (CFIT 2024, p. 8).

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 can create 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 businesses, 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 – for instance, 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 require significant upfront investment and ongoing costs, especially for firms with fragmented or outdated back-end systems (ABA 2020b, p. 10; Accenture 2024a, p. 24; Treasury 2021, p. 7, 2023a, pp. 10–12). For example, firms may need to invest in their data security and cyber-defence capabilities to mitigate any increased risk of cyberattacks or data breaches which can result in major disruptions, large fines and reputational harm (Gao et al. 2025, p. 1; Liu and Babar 2024, pp. 11–17).

But many firms do voluntarily provide their customers with some means of accessing the data they hold about them. This can occur in response to consumer expectations or to keep up with their competitors, as has occurred in the agricultural sector (appendix E). Where firms compete in adjacent markets or have complementary offerings, allowing their customers to easily move data between their services can make each product more useful (OECD 2021, pp. 19–26). For example, Fitbit, Apple and Garmin all allow users to sync the activity data (such as daily steps and heart rate) from their smart-watches with third-party platforms

such as Strava (Allison 2025; Scott 2024). Similarly, businesses who use Square's Point of Sale terminals and Xero can link their accounts to enable sales transactions to be auto-posted daily to their general ledger (Square 2022). For some digital platforms, allowing consumers to share and integrate data across a diverse range of related services is a key part of their business model.

> the business reality for enterprise SaaS (Software as a Service) companies like Workday is more nuanced. For organisations that have made a significant investment to transit to and integrate with a platform like Workday, they are typically less likely to switch vendors as they recognise that the value extends far beyond simply possessing their data. It lies in the interconnectedness and functionality of that data within a unified system. (Workday Australia, sub. 309, p. 4)

Data access constraints can result in material costs

When individuals and businesses cannot access data directly, they often resort to re-collecting or regenerating it (box 3.2). This results in lower productivity through duplication and waste and can actively lead to consumer harm. For example, a person who cannot transfer their existing medical data to a new provider may have to redo X-rays, which comes with a financial cost, heightened health risks and delays to their diagnosis and treatment.

Box 3.2 – 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 for individual outcomes and for productivity.

- 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).

Consumers can also turn to unofficial or third-party tools and solutions to independently tap into the data from the products and services they use (CCAF 2024, p. 20; OECD 2021, p. 12). These tools include auxiliary 'data loggers' that plug into hardware to capture operational data (such as dongles that connect to vehicle diagnostic ports to access telematics data) and screen scraping applications that programmatically extract data from user accounts or portals by using their login credentials (CCAF 2024, p. 20; OBD2 Australia 2025; 2023b, pp. 5–6).

While these alternative access mechanisms can be highly useful, they can also be unreliable and insecure (CCAF 2024, p. 20). Original providers will often try to deter their customers from using them and can intervene to disable them (OECD 2021, pp. 7, 14). This can take the form of technical blocks (like disabling access ports

or throttling connection speeds), imposing paywalls (including to access an API) or legal sanctions[25] (including declaring terms of service violations and voiding product warranties) (OECD 2021, pp. 26–34; Treasury 2023b, pp. 6–8). Tools such as screen scraping can also increase the risk of cybersecurity or data breaches. Screen scraping can potentially provide a third party with unfettered access to a consumer's account on an ongoing basis and without their knowledge or control (Treasury 2023b, pp. 6–7). This can increase their vulnerability to fraud – the Commonwealth Bank of Australia found that customers who use screen scraping are at least twice as likely to experience fraud on their accounts (Eyers 2020). Moreover, under the ePayments Code, a bank can refuse to reimburse a customer for losses if they have shared their passcode (ASIC 2022, p. 16).

Government can help to facilitate data access but industry will often be well-equipped to enable it

Governments can play an important role in facilitating data access where efficient data markets are unlikely to develop. For example, open banking initiatives like the CDR – which operate in some form in 60 countries around the world – often rely on mandatory data sharing requirements (CCAF 2024, p. 56). The Global State of Open Banking report found that mandatory data sharing obligations have been necessary in many jurisdictions to initiate data sharing in their banking sector (CCAF 2024, pp. 41–49).

However, a one-size-fits-all approach is unlikely to deliver intended outcomes across the board – high-value use cases in different sectors will depend on varying types of data, access mechanisms and security controls. The CDR sets broad, prescriptive rules for how data must be shared (Treasury 2025b, pp. 8–10). While this approach carries benefits, like ensuring data access is highly secure, the trade-off can be high compliance costs for businesses and a stymieing of innovative use cases (Treasury 2023a, pp. 16–17).

The overspecification of the CDR framework is preventing it from operating as intended

The CDR was intended to function as an economy-wide data access scheme with the aims of promoting competition and encouraging innovation that will benefit consumers via better products, lower prices, and access to third-party tools (Australian Government 2025e; Treasury 2022b, pp. 45, 85).

To date, the CDR's implementation has been slow and costly. The banking industry reports that it has spent $1.5 billion implementing the CDR, with costs for data holders ranging from under $1 million to well over $100 million each (Accenture 2024a; Treasury 2023a, pp. 2–3). A significant driver of costs has been the CDR's binding data standards that have continuously been revised (Treasury 2023a, p. 3). Over 20 versions of these standards have been introduced since the rollout began in mid-2020 (Treasury 2023a, p. 3).

Another challenge – exacerbated by the CDR's high costs – has been gaining the good faith cooperation of incumbent data holders. Treasury has observed that some incumbents may see the scheme as a threat to their interests and that their attempts to minimise their own implementation costs 'can result in negative outcomes for the entire ecosystem, including poor quality data, inconvenient processes for consumers and limited cooperation in resolving issues' (2025b, pp. 9–10).

---

[25] 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 there may be legal implications including under privacy, copyright and/or contract law.

In August 2024 the Australian Government announced a 'reset' of the CDR that would focus on minimising issues like high implementation and compliance costs in an attempt to make the CDR more appealing to consumers (Jones 2024a). The government has made several targeted changes to the CDR, including:

• reducing the period that data must be shared and retained from seven to two years
• removing requirements on sharing 'niche' product data
• enabling consumers and businesses to agree to multiple consents in a single-step and simplifying the information that needs to be included in the consent process (Australian Government 2025c, p. 37; Jones 2025).

The scheme is now starting to make headway. In the six months to June 2025, the CDR has been used by about 821,000 consumers to serve 741 million data requests (ACCC, sub. 495, p. 6), an increase of 55% in consumers served from the reporting period earlier (figure 3.2).[26] If this current uptake trend continues, the CDR will be on track to surpass one million consumers served during the next reporting period. 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, p. 5,17).

Figure 3.2 – CDR uptake
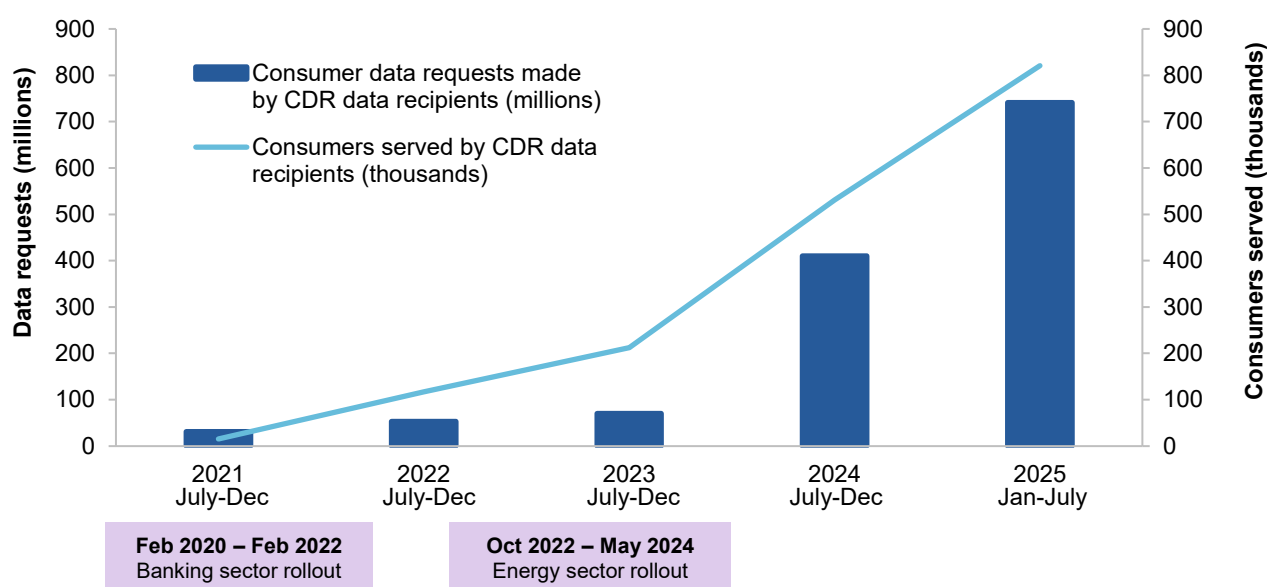
Source: ACCC, sub. 495, p. 7.

As part of the CDR 'reset', the government has moved to bring non-bank lending products into the CDR (which were initially designated in 2022) starting from July 2026 (Australian Government 2025b; Jones 2025). But despite being established as an economy-wide scheme, the government has paused the expansion of the CDR into new sectors, such as telecommunications (which was designated in 2022) or superannuation and insurance (which were previously identified as priorities) (Australian Government 2023).

A key issue is that the CDR has limited capacity to distinguish between different types of use cases and datasets or be tailored to the market dynamics and technological capabilities of different sectors. While its operational rules (such as its eligibility criteria) can be tailored for different sectors (ACCC 2025c;

---

[26] These figures may overstate the number of 'unique consumers' who have used the CDR. Consumers may be double counted if they cancel a consent or let it expire and then submit a new consent, and an ADR does not identify them as the same individual.

Treasury 2025a), core parts of the CDR's architecture are mandated (box 3.3). This includes its accreditation model, privacy safeguards and technical standards. Despite the reset, the set-up costs of these features still impose a relatively high bar for bringing new sectors into the scheme.

Box 3.3 – The architecture of the Consumer Data Right

The Consumer Data Right (CDR) is a regulatory and technical framework that enables consumers to consent and share data with accredited third parties in a safe and interoperable way.[a] When a sector is designated, it is formally brought under the CDR framework. This designation specifies which datasets and participants are covered and requires designated data holders to share consumer data with Accredited Data Recipients (ADRs) when requested by a consumer. It also triggers the development of sector-specific rules, data standards, and compliance obligations. The CDR has several key building blocks:

- **Technical standards** – Data holders must comply with the operational and security requirements for data sharing. Developed by the Data Standards Body, the standards are designed to ensure consistent authentication, encryption, and data formatting across sectors, with the aim of achieving secure and interoperable exchange of consumer data.
- **Accreditation System –** Entities seeking access to consumer data must obtain accreditation through the Australian Competition and Consumer Commission (ACCC). The accreditation process is focused on security, governance, and privacy standards to ensure ADRs are accountable and capable of handling consumer data safely within the CDR framework. The CDR offers full accreditation, and sponsored, representative, and outsourced service provider access that lets entities that are not accredited operate under an accredited party while maintaining core privacy and security standards.
- **Register –** The ACCC maintains a central, publicly accessible database of ADRs and provides technology to underpin the security and transparency of the CDR by ensuring data is only shared between verified, accredited participants.
- **Bespoke Privacy and Data Protections** – Stringent privacy and consent safeguards – such as explicit, time-bound consent and strict data request, use and deletion requirements – apply to all organisations handling CDR data. Enforced by the Office of the Australian Information Commissioner, these safeguards ensure CDR data is subject to uniform privacy and data protection standards, regardless of whether entities are regulated by the *Privacy Act 1988*.

Box 3.3 – The architecture of the Consumer Data Right

Part IVD of the Ccompetition and Consumer Act

Minister	Treasury
Responsible for designating sectors	Responsible for making the CDR rules

Designation instrument	CDR Rules
Outlines which sector and data to be included	Legislative instrument that sets out how CDR operates

CDR infrastructure applied to designated sectors

Technical standards	Accreditation system	Public register	Privacy and data protections
Set by a government setting body	Limits immediate access to ADRs	Certifies ADRs to support safe data sharing	Bespoke privacy and data protections for CDR consumers
DSB	ACCC		OAIC

a. Although the CDR framework was designed to enable both data sharing with third parties and direct consumer access to data about themselves, the direct consumer access function has not been implemented in any sector.

Source: ACCC (2025c; 2025b), Australian Government (2025a), Treasury (2025a).

For data access, a light-touch approach often works

Data regulation needs to be flexible. 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 case to case. Regulation also needs to recognise that the costs of providing access can vary significantly depending on what data holders need to share and how.

Some data use cases only require a light touch, but the payoffs can still be large. A basic capability to export data in a machine-readable format is often sufficient for consumers to realise significant gains. For example, existing budgeting, meal planning and lifestyle apps can often require users to manually enter in transaction or consumption data (CHOICE 2025). Enabling consumers to upload (rather than manually type out) their historical purchases into these apps, can make it easier for consumers to track their spending, identify savings opportunities, and make healthier choices.

To this end, our interim report outlined an industry-led approach to basic data exports that would enable individuals and businesses to access relatively non-sensitive data on a periodic, or ad-hoc basis. We indicated that this form of access could be facilitated through sector-specific data access codes and potentially at minimal cost, particularly where firms in the sector already provide their customers with access to a secure online account or portal. As an example, the PC has looked at current data access and sharing practices of retail loyalty and rewards programs (box 3.4).

Box 3.4 – Data access and sharing in the retail loyalty sector

Loyalty programs can accrue rich information sets about consumers including about their shopping purchases, patterns, preferences and broader interests (ACCC 2019, pp. 49–52). This information can be used by the retail business directly or shared with third parties, to tailor customer experiences, target advertisements and make product recommendations.

Consumers can access some of this data. For example, it is commonplace for 'bricks and mortar' retailers and loyalty providers to allow consumers to download data about their purchases through their online digital portals, typically in the form of a PDF digital receipt. This is far from frictionless access: stitching together a time series requires downloading multiple PDFs, which are not machine readable.

There are more and more third-party tools …

A variety of unofficial third-party tools have emerged to make it easier for consumers to access and share data about purchases. Those who are relatively tech savvy can use screen scraping to enable bulk data capture (for example MyShopDash and WooliesR). Those with less technological nous can use apps like Wiselist – an Australian grocery comparison app – which enables consumers to take photos of receipts and scan barcodes to facilitate price comparison and meal planning (WiseList 2025a, 2025c, 2025b).

… and native data access offerings are also improving

Loyalty program providers and third-party platforms are developing features that allow users to link their accounts directly with other services. For instance, Woolworths Group allows Everyday Rewards members to link their accounts with other platforms within its ecosystem, such as Healthylife, to receive personalised health and nutrition insights generated from shared transaction data (Healthylife 2025).

AI is entering the field …

To deal with a lack of standardised data fields and naming conventions between retailers, such as for product names, price comparison tools such as Grocerize – an Australian tech company – are leveraging AI-matching tools to facilitate price comparisons between major grocers (Grocerize 2025c, 2025a).

Overseas, some retailers are developing integrations that allow their customers to connect their digital accounts to generative AI tools. For example, Walmart – a US retailer – has partnered with OpenAI to enable shopping through ChatGPT (Walmart 2025). This capability has been extended to online merchants Shopify and Etsy (OpenAI 2025b). Product information from multiple retailers – such as prices, availability, specifications, and reviews – is integrated into the ChatGPT interface, while consumer data, including expressed preferences and past interactions, informs personalised recommendations across different retail platforms.

… screen scraping with low-risk data opens up further possibilities

In the United States of America, the app Cooklist enables consumers to aggregate data across accounts with different retailers, including Walmart, Kroger, Safeway, Amazon, and Target. It uses permissioned screen scraping to automatically import purchases into a digital pantry, make recipe recommendations based on available ingredients and generate shopping lists (Cooklist 2021, 2025).

The PC heard from some participants who suggested that a 'light handed' data access pathway already exists. They pointed to the Privacy Act, which under Australian Privacy Principle (APP) 12, already requires data holders to provide individuals with basic data access. However, APP 12 is not designed to facilitate the

creation of a data portability scheme: it applies only to personal data, requires individuals to make specific requests, it does not require that data is provided in a machine-readable form, and its remit does not cover product data or business information. Even so, an obligation of this sort in the Privacy Act (chapter 4) signals to data holders the importance of providing consumers with relatively straightforward ways to access their basic data, which can serve as a gateway to broader data sharing.

Our case studies highlighted how data access functionality is actively evolving. Even when direct access is limited, intermediaries and third parties are developing solutions that allow consumers to bring together non-standardised or unstructured data that is available from the products and platforms they use (box 3.5). This creates an ecosystem that supports more effective data access and use over time, a process likely to accelerate with the development and adoption of agentic AI tools.

Box 3.5 – 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) to support different use cases (WEF 2022, pp. 9–10). Two examples are service-to-service models and Personal Information Management Systems (PIMSs).

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 from one service to another (DTI 2018, pp. 5–6). In contrast, PIMSs, 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 in user-friendly dashboards, enhancing its quality or enriching it with analytics (OECD 2019, p. 36). For example, Apple's Health app allows iPhone users to analyse trends and generate insights that can be shared with healthcare providers (Apple Inc. 2025).

There are emerging data access solutions that rely on screen scraping to retrieve information from user accounts or online portals. For example, tools such as Storelink enable developers to integrate account-linking flows into their apps so that users can log in to their retail accounts and share itemised transaction records (Storelink 2024a, 2024b). However, screen scraping can also create privacy, security, and compliance risks, particularly when users must share login credentials or when scraping occurs outside authorised channels (Treasury 2023b).

The Australian Government has sought advice from Treasury on how to progress 'a full and formal ban of screen scraping' (Jones 2024b). This follows a consultation process in 2023 that sought feedback on banning the practice in sectors where the CDR provides a viable alternative (Treasury 2023b). Both the Australian Competition and Consumer Commission (ACCC) and the Office of the Australian Information Commissioner (OAIC) supported the proposal (ACCC 2023, p. 2; OAIC 2023c, p. 1), noting the 'significant privacy and security risks' that screen scraping can pose for individuals (OAIC 2023c, p. 1). 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 PC considers that an outright ban on screen scraping in the absence of an effective substitute is premature. A blanket ban is a blunt regulatory instrument, and in cases where the risks are low (such as scraping from relatively non-sensitive data), consumers can benefit from being able to access and use their data via tools that rely on screen scraping.

Removing constraints on high-value applications of the CDR in existing sectors

Notwithstanding the recent changes made under the Australian Government's CDR reset, overall progress on improving the CDR has been slow and piecemeal. Many inquiry participants reiterated that they are subject to restrictive and cumbersome rules (ARCA, sub. 366, p. 10; ATA, sub. 317, p. 6; BCA, sub. 488, p. 7; Data Synergies, sub. 411, p. 2; FinTech Australia, sub. 578, p. 9). These rules continue to obstruct high-value uses of the scheme. The main issues they identified are well-known and have been examined by previous reviews and consultation processes (Treasury 2022b, pp. 45–46, 2023a, p. 7,11, 2024a, pp. 8–9). They include:

- manual onboarding processes that make it difficult for small and medium-sized enterprises (SMEs) to participate
- consent rules that limit consumer sharing of data with third parties
- limits on how CDR data can be used.

Inquiry participants emphasised the need to prioritise reforms to simplify the CDR and remove constraints that are inhibiting its potential. This included support for progressing with targeted rule changes that are currently under consideration and could be implemented in the near term (box 3.6).

Such changes could open a wider range of uses for the existing datasets that can be shared through the scheme. For instance, the Department of Finance and Treasury are currently undertaking a pilot to use the CDR and Digital ID to provide an easier and safer way for people to apply for rental properties (Gallagher et al. 2025). Rather than having to provide copies of their identity documents and bank statements or payslips to real estate agents, applicants will be able to use their Digital ID to verify their identity and their CDR banking data to demonstrate they can afford the rental payments on a property.

> For renters, it means more control over where their data goes, better peace of mind when sharing personal data and fewer forms to fill. For property managers, it means less admin and more confidence that the information they're receiving is accurate (PropertyMe 2025)

The rental pilot is a good example of the digital innovation the CDR was intended to deliver, and how it can complement and operate alongside other components of Australia's digital public infrastructure (ACCC, sub. 495, p. 11).

While the consortiums participating in the pilot (each consisting of a Digital ID provider, Accredited Data Recipient (ADR) and real estate business) are testing various technical solutions, the CDR's current disclosure rules may prevent ADRs from being able to on-share the necessary data with real estate agents. More generally, the pilot highlights the importance of having agile mechanisms to road test and adjust the CDR's rules to ensure they are not inhibiting high-value use cases.

Box 3.6 – Opportunities to improve the Consumer Data Right (CDR) in the short term

Complicated on-boarding processes for business consumers

For a business to access and share data via the CDR, it often must first appoint a nominated representative (an individual authorised to manage data sharing on the business's behalf). Data holders have implemented varying processes that businesses must follow to make this appointment, which can require the completion of multiple paper-based forms and in-person identity checks (ACCC, sub. 495, p. 10; Treasury 2024a, p. 10; Xero, sub. 355, p. 8). This involves duplicative effort for businesses who typically have already taken steps to appoint an 'administrator' who is authorised to manage their online accounts.

By overcomplicating the initial on-boarding experience, the nominated representative process discourages SMEs from using the CDR and has contributed to high on-boarding failure rates (FintTech Australia, sub. 578, p. 9). Xero (sub. 355, p. 8) - a cloud-based accounting platform - submitted that for small businesses, the process is '*confusing, time-consuming, and at odds with the very goal of streamlining data access*' and the ACCC (sub. 495, p. 10) acknowledged it is 'considered a key barrier to greater business participation in CDR'.

Proposed solution: Submissions from the ACCC and industry participants recommended modifying the nominated representative rules to give individuals with existing authority on an online business account equivalent authority to consent to data sharing via the CDR (ACCC, sub. 495, p. 10; FinTech Australia, sub. 578, p. 9, Xero, sub. 355, pp. 7–8). The PC understands that Treasury is currently considering potential approaches to implement this change, following a decision not to proceed with an earlier version that was consulted on in 2024.

Limitations on data disclosure

As discussed above, the CDR imposes tight controls on how data can be shared and used under the scheme. The current rules only permit consumers to share data for specific purposes using 'situation specific' consent types (for example, trusted adviser consents and business consumer disclosure consents). Moreover, once shared CDR data generally continues to carry scheme-specific restrictions (including limits on using information 'derived' from CDR data).

These restrictions constrain how CDR data can be put to use. For example, the personal finance app, WeMoney (sub. 597, p. 19), noted that consumers who have shared data with them via the CDR are unable to easily on-share it with lenders to support loan or refinancing applications. Similarly, Xero (sub. 355, p. 9) submitted that the CDR's derived data rules prevent small businesses from using CDR data in basic tools such as reconciled transactions or cash-flow forecasts.

Proposed solution: The PC understands that Treasury has undertaken a targeted consultation process on the introduction of a third-party disclosure consent that would enable consumers to direct an ADR to disclose their CDR data to any third party of their choosing. Once shared with the third party, the data would be subject to the Privacy Act rather than CDR's privacy safeguards. FinTech Australia (2025a, pp. 20–21) has proposed that as well as enabling additional use cases, the change could reduce the scope of data standards that need to be maintained and support integration with Digital ID.

The government should commit to enacting more substantive changes …

In addition to these targeted measures, inquiry participants submitted that more substantive changes are needed.

One of these changes is reducing duplication between the CDR framework's bespoke privacy safeguards and the privacy protections under the Privacy Act, an issue raised in the 2022 *Statutory Review of the Consumer Data Right*.[27] The CDR's privacy safeguards currently subject data shared via the CDR to more stringent handling requirements and usage restrictions than if the same data is accessed under the Privacy Act. Participants in this inquiry characterised the bespoke treatment of CDR data as 'the biggest single barrier to participation' (Mastercard (Australasia), sub. 775, p. 2) and a driver of the ongoing use of screen scraping (FinTech Australia, sub. 578, p. 9). The impacts of the CDR's privacy settings were also highlighted by the scheme's joint regulators.

> CDR participants are required to comply with its bespoke privacy regime, creating cost and complexity to maintain two separate privacy systems for CDR and non-CDR data. (ACCC, sub. 495, p. 10)

> The OAIC would also support measures to ease regulatory burdens on CDR participants by streamlining laws to avoid duplication between primary privacy legislation and bespoke CDR privacy obligations, through the adoption of the Privacy Act as the sole regulatory regime. (OAIC, sub. 356, p. 7)

There have been some recent reforms to the Privacy Act, and it is anticipated that further reforms will take place (chapter 4 and appendix F). The PC considers that the Privacy Act should operate as the primary piece of legislation in Australia to effectively protect individuals' information privacy (box 4.1 in chapter 4) in data sharing schemes like the CDR. This would remove the need for the CDR to have bespoke privacy settings and eliminate duplication with the Privacy Act.

A second change is enabling government-held datasets to be accessed through the CDR. This was recommended by the 2022 Statutory Review of the CDR to ensure consumers could 'benefit from more seamless government interactions and an ability to share their data across a greater range of services' (Treasury 2022b, p. 62).

The PC heard from industry participants who indicated that the inclusion of relevant government datasets could enhance the productivity benefits achievable from the scheme (MFAA, sub. 532, p. 7; WeMoney, sub. 597, p. 25; Westpac, sub. 413, p. 2). Both Westpac and the Mortgage and Finance Association of Australia (sub. 532, p. 7) noted that the inclusion of Australian Tax Office (ATO) data in the CDR could help improve access to credit.

> integrating government data could dramatically speed up loan applications by reducing the need for manual documentation and verification, which is cumbersome for both the customer and the bank and presents ongoing personal data storage risk. (Westpac, sub. 413, p. 2)

International experience points to similar benefits. A pilot study in the United Kingdon demonstrated that the integration of Value Added Tax (VAT) data in the country's Open Banking scheme could reduce SME loan

---

[27] The 2022 Statutory Review of the Consumer Data Right made no recommendations in relation to the Privacy Act and the CDR creating dual requirements for participants of the CDR. The Review found that 'protections provided by the CDR are designed to ensure the integrity of the scheme is maintained as it moves across each sector working alongside the Privacy Act 1988' (Treasury 2022b, p. 63). Where opportunities for alignment with the Privacy Act 1988 are identified, the CDR protections should be reviewed to reduce duplication and increase alignment'.

application times by half and increase loan offers by 20-40% (CFIT 2024, pp. 16–17). Several other countries including Singapore, India and Estonia have already incorporated government-held data into their data access regimes (Deloitte 2023, pp. 16, 26; GovTech Singapore 2025).

In their submission, the ATO acknowledged that enabling individuals and businesses to authorise the sharing of their tax data through the CDR could enhance 'transparency, personal agency, and service delivery' (ATO, sub. 776, p. 4). However, it emphasised that consent-based data disclosure is currently not permitted by the strict confidentiality restrictions within the *Taxation Administration Act 1953* (Cth). In 2024, as part of a review of the tax secrecy exceptions, Treasury sought feedback on introducing an amendment that would allow taxpayers to directly share their data with third parties (Treasury 2024b, p. 39). As of November 2025, the outcomes of this review have yet to be announced. Provided the review does not identify any risks that cannot be adequately mitigated, the government should progress this amendment at the earliest opportunity and direct Treasury to work with the ATO to design and assess a targeted designation approach that will allow consumers to securely share their tax data through the CDR.

... but must avoid undermining incentives to participate in the CDR

A key focus of the Australian Government's 'reset' of the CDR is to make it less costly for businesses to participate in the scheme (Jones 2024c). While measures should be taken to minimise compliance costs where possible, it is critical that these efforts do not inadvertently dilute the productivity benefits that could be achieved through use of the scheme.

Industry participants have raised concerns in relation to Treasury's targeted consultation on removing the data sharing obligation for small banks. The proposed exemption would allow 'authorised deposit-taking institutions' (ADIs) with total assets of less than $5 billion to opt out from the CDR; the proposal estimates this threshold would apply to 55 ADIs and leave 22 ADIs with mandatory CDR obligations (MFAA 2025, p. 3). While the PC understands that the remaining banks account for 98% of existing data sharing contracts, stakeholders have argued that the change would undermine the value of data sharing under the scheme and disadvantage small bank customers.

> This proposal poses a risk to the foundations of Open Banking … The power of this pro-competition regime is its universality, which empowers consumers, drives innovation and preserves competition (Rehan D'Almeida, CEO, FinTech Australia 2025b)

> The CDR is at a turning point. Brokers — who originate most Australian home loans — have just gained universal access, and consumers are starting to experience faster, safer ways to share financial data. Introducing a de minimis threshold now would fragment coverage, slow adoption, increase costs across the system and push some customers back to the use of insecure screen scraping. (MFAA 2025, p. 4)

The viability of many high-value use cases of the CDR in the banking sector rely on it being able to provide a single and secure access point. Given this, the PC cautions against changes that would permit some banks to opt out (and so prevent their customers from being able to securely share data through the scheme) of what is meant to be a whole-of-sector data sharing initiative. There is a risk that ad hoc carveouts could undermine the integrity and overall value of the CDR.

Deferring features that could enhance the CDR's functionality, such as 'action initiation' (also known as 'write access'), also risks hampering the scheme. Action initiation allows consumers to direct third parties to perform actions on their behalf, such as automating payments, updating personal information, and switching,

opening or closing accounts. Legislation[28] was passed in August 2024 to enable action initiation under the CDR framework, but the government indicated at the time that it 'will not rush' to implement the capability 'until the CDR is back on track' (Jones 2024a).

International experience shows the potential significant upsides for action initiation. The 2024 Global State of Open Banking report finds that it 'significantly enhances the potential for innovative and impactful financial services' and notes that 55 jurisdictions have enabled it (CCAF 2024, p. 51). In the UK, action initiation has helped drive open banking adoption by supporting a broad suite of payment services (Open Banking 2025). Participants suggested it could have similar benefits in Australia: WeMoney (sub. 597, pp. 23–24) submitted that its absence 'is a key limiter to the CDR's growth' and that implementing it would 'dramatically expand the functionality' of their platform, while FinTech Australia (sub. 578, p. 9) indicated it could enable future agentic AI use cases.

A 'lighter-touch' CDR is needed to enable a wider range of high-value data access use cases

Not every data use case should be subsumed into, or regulated by the CDR. However, if the CDR is to have the potential to function as an economy-wide scheme, it needs to be able to accommodate the structural characteristics and the level of digital maturity of different sectors. The latter can vary widely. Several participants in this inquiry agreed with the PC's assessment that the CDR is currently ill-suited for most data access use cases.

> the existing CDR framework is too complex and prescriptive for most data access applications: it is not a suitable starting point to address safe and secure access for most non-financial consumer transaction data sets. (Peter Leonard, sub. 411, p. 2)

> The CDR is currently unworkable as a data sharing model. It is unwieldy and, as the PC recognises itself, its accreditation model, bespoke privacy safeguards, and technical requirements are too onerous. (BCA, sub. 488, p. 7)

While participants broadly endorsed the intent of establishing lower-cost and more flexible regulatory pathways to expand data access – as described in the PC's draft recommendation – many argued that it would be more easily achieved by amending the CDR.

> in our view it would be simpler and more efficient to build upon the data sharing infrastructure we already have – the CDR. The CDR was always intended to serve as an economy-wide data sharing framework (Mastercard (Australasia), sub. 775, p. 3)

> Given the challenges and risks with developing alternative pathways, we suggest leveraging the strong data-sharing fundamentals Australia has already built to generate more value for consumers and business would be better for productivity and minimises duplication, disconnect, and waste. (ACCC, sub. 495, p. 13)

> The TCA (Tech Council of Australia) advocates for the use of existing mechanisms, such as the Consumer Data Right (CDR), for improved access to data in sectors with a demonstrated data access deficit. To enable this, it is critical that the shortcomings in the design of the current CDR system be addressed. (TCA, sub. 543, p. 15)

---

[28] *Treasury Laws Amendment (Consumer Data Right) Act 2024* (Cth).

The PC acknowledges that the creation of new access pathways could add to existing regulatory complexity and data policy fragmentation without providing a net improvement in productivity outcomes for the economy. And as discussed above, based on consultation in this inquiry, the PC does not see a clear case for creating regulatory pathways or new data sharing regulations.

Instead, we support rightsizing the existing CDR framework so that it has the potential, where necessary, to be used for a broader range of sectors and productive uses (for instance, if market structure or technological factors are inhibiting the development of data access solutions for consumers).

At a basic level, rightsizing the CDR could entail, for designated use cases, defining which firms need to share data, what they need to share, and how. Additional blanket requirements should be kept to a minimum. This is because, provided the relevant data can be reliably accessed through a suitable mechanism, intermediaries and third parties can develop adaptors and integration services to effectively handle variable data standards. Experience in the agricultural sector bears this out (box 3.7). The government should also avoid setting requirements that go above and beyond existing legislation, such as the Privacy Act (discussed above).

Box 3.7 – Farmers can largely access the data they need

Farmers use data about their farms for a variety of purposes. Equipment and machine data is particularly useful to farmers as it can be downloaded to analyse farm production and uploaded to machines or passed between bits of equipment to direct the machinery. Historically, this has been difficult. Data often had to be manually transferred using USBs and SD cards. A lack of common exchange standards made it difficult to compile and analyse data from various sources. And in some cases, proprietary interfaces meant that farmers had to install multiple dedicated joysticks and screens to use different machinery attachments such as seeders, sprayers and balers (AEF 2015, p. 9; Aspexit 2021; Keogh and Henry 2016, p. 27).

A tractor without ISOBUS (left) vs. one with ISOBUS (right)

Source: Olliver et al.

Over time, access to machine data has improved in the sector. Strong demand from farmers and machinery users for interoperable data solutions has prompted a variety of responses from manufacturers (Keogh and Henry 2016, pp. 27–28; 2023, pp. 3, 7). These include the creation of APIs by manufacturers to enable easier access to machine data, manufacturers grouping together to implement common data standards for cross brand interoperability and the emergence of third-party service providers.

The Agricultural Industry Electronics Foundation (AEF), formed in 2008, is an example of an effective sectoral response to consumer (farmer) demand for data access. The AEF is made up of eight international agricultural equipment manufacturers (including John Deere, CNH and AgCO) and three associations (and

---

Box 3.7 – Farmers can largely access the data they need

over 300 general members) and supports the development and implementation of common data standards (AEF 2025a, 2025b). The AEF has advocated for the adoption of the ISOBUS interoperability protocol, which enables equipment from different manufacturers to integrate and work together reliably.

ADAPT (Agricultural Data Application Programming Toolkit) is an open-source common data model and software toolkit that supports the conversion of machine and equipment data between proprietary formats (AgGateway 2025a). ADAPT was developed by AgGateway, an industry association with a membership made up of manufacturers, software providers and retailers (AgGateway 2025b).

In Australia, Pairtree is an agtech company that provides a unified dashboard and integration-engine for farm data (Pairtree 2024b). Its services aggregate and standardise data feeds from multiple devices, portals and digital services (weather, sensors, market data, satellite imagery etc), enabling farmers and agribusinesses to visualise, compare and analyse disparate data sets in one log-in space.

But a Right to Repair is needed to ensure access to diagnostic data

Previous reviews by both the PC and ACCC found that there are restrictions on diagnostic data, software and tools required to maintain and repair farm machinery, and the National Farmers' Federation's Right to Repair taskforce have argued that these issues have not improved (ACCC 2021, p. 39; NFF 2025; PC 2021, p. 138). In November 2025, the Australian Government announced that it will extend Right to Repair reforms to agricultural machinery as part of an updated National Competition Policy Agreement (Chalmers 2025).

Data sharing in the agriculture sector is explored in appendix E.

Changes could be made to the accreditation model, technical standards and designation process

In addition to aligning the CDR with the Privacy Act, a lighter-touch approach would likely require amendments to the scheme's accreditation model, technical standards and sectoral designation approach.

A lighter-touch accreditation model

Gaining accreditation to directly receive CDR data from data holders requires passing a fit-and-proper person assessment, having robust and independently assured data security controls, belonging to an external dispute resolution scheme and holding adequate insurance (ACCC 2025a, pp. 15–21). On an on-going basis, Accredited Data Recipients (ADRs) must provide dashboards that enable consumers to manage their consents, adhere to strict record keeping requirements and submit biannual operating reports to the ACCC and OAIC (Australian Government 2025d; OAIC 2025a). The 2022 Statutory Review of the Consumer Data Right heard that these requirements are expensive and complex to meet and can duplicate similar accreditation processes that businesses have already undergone (for example Digital Service Providers registered with the ATO) (Treasury 2022b, p. 49).

The Business Council of Australia (sub. 488, p. 7) proposed that the CDR should be 'dramatically' simplified with data recipients being accredited to minimum cyber standards and consumers having the power to consent to data sharing as they wish. While the introduction of a 'third-party disclosure consent' should make it easier for consumers to share data as they wish, the scheme's accreditation model will remain too onerous for many use cases. This is likely to be the case in sectors where consumers want to be able to directly

share data with SMEs or where intermediaries are already receiving and processing data on behalf of consumers (for example the agricultural sector).

An alternative approach could see the CDR's current accreditation model used for highly-sensitive datasets (for example income tax or health records). For datasets that are less sensitive or routinely shared in some form (for example retail loyalty data), consumers could be allowed to authorise their data to be directly shared with entities that are already subject to the Privacy Act and other relevant sectoral regulations.

Technical standards that are fit-for-purpose

To operate as an economy-wide data access scheme, the rules and technical standards of the CDR must be able to be tailored to the requirements of diverse use cases. As they stand, the CDR data standards aim to ensure consistency across sectors with respect to authentication methods, security requirements, status reporting and API performance (including its reliability, response times and traffic capacity). This is intended to facilitate the 'seamless' integration of data from multiple sectors and 'to reduce the cost of customer education for new sectors' (Data Standards Body 2025). Some participants cited these aims as an argument against establishing new data access pathways. For example, the Law Council of Australia (sub. 599, p. 18) suggested 'integrating multiple sectors under unified data sharing rules offers a substantial volume of standardised data that can be harnessed for innovative applications'.

However, experience to date suggests that the benefits of this level of standardisation are unlikely to outweigh the costs. While some use cases may require drawing together data sets from distinct sectors, provided consumers can access and share the data needed, intermediaries are likely to develop tools and services to aggregate it. In contrast, the costs of conforming to uniform technical requirements will render many use cases unviable and result in consumers resorting to less secure access mechanisms.

In general, the way in which use cases are 'solved' (for example, via a technical solution imposed by industry, government or an independent data standards body) needs to take account of the different capabilities of data holders and the costs (and who bears them and how) of implementing preferred solutions.

A more targeted designation approach

To date, the CDR has been implemented by assessing whole sectors (banking, energy and telecommunications) and designating as in scope, a broad collection of datasets.[29] Participants in this inquiry said that this broad approach 'has led to significant uncertainty and lengthy lead times for new sectors to be designated' (WeMoney, sub. 597, p. 33), and the 2023 *Consumer Data Right Compliance Costs Review* found that the regulatory impact analyses for existing sectors had significantly underestimated implementation costs (Treasury 2023a, p. 2,9).

An alternative approach, suggested by several reviews and studies, is a much more targeted, data or use-based (rather than sector based) approach to expanding the scheme. For example, the 2022 Statutory Review of the Consumer Data Right endorsed a designation approach that gives greater focus to use cases and saves data holders from having to 'overhaul systems for low-value CDR datasets or bespoke products' (Treasury 2022b, p. 21). With respect to its expansion into Open Finance[30], Treasury's *Strategic Assessment* of the CDR (2022a, p. 8) concluded that prioritising a small number of targeted datasets would 'unlock a broader range of higher value use cases, compared to expanding one sector at a time'. Similarly, Deloitte

---

[29] Sectoral assessments currently require the Treasurer to consider the likely effects on consumers, market efficiency, competition, privacy and confidentiality, data-driven innovation, intellectual property, the public interest and the potential regulatory impact (Treasury 2022b, p. 88). It also requires Treasury to undertake public consultation on the assessment and draft designation and consult with the ACCC, OAIC and relevant sector regulator.

[30] Defined as including the general insurance, superannuation, merchant acquiring and non-bank lending sectors.

(2024a, p. 3,46) has argued for a 'consumer-centric' approach that allows cross-sectoral datasets to be designated that can support use cases tied to key life events.

In practice, a more targeted and agile designation approach would start with the minimum viable dataset needed to support established use cases and allow additional data fields to be phased in once further benefits and technical feasibility is evaluated. Under this model, data holders could also be given greater scope to offer extended data access, on a voluntary or commercial basis, such as additional data fields, higher-performance service levels or value-added analytics. The assessment process could also be refined to focus on validating consumer demand and implementation costs by mapping existing data sharing practices and technological capability. As submissions from the Business Council of Australia and CSIRO suggest, this should involve extensive engagement with industry participants and the use of pilots and sandboxes to test feasibility (BCA, sub. 488, p. 9; CSIRO, sub. 322, p. 8).

» **Recommendation 3.1**
Rightsize the Consumer Data Right

The Australian Government should commit to reforms that will enable the Consumer Data Right (CDR) to better support data access for high-value uses while minimising compliance costs.

In the short term, the government should continue to simplify the scheme by removing excessive restrictions and rules that are limiting its uptake and practical applications in the banking and energy sectors. To do this, the government should:

- within the next two years, enable consumers to share data with third parties and simplify the on-boarding process for businesses
- commit to more substantive changes to the scheme (in parallel with related legislative reforms), including aligning the CDR's privacy safeguards with the Privacy Act and enabling access to selected government-held datasets through the scheme.

In addition to the above, the CDR framework should be significantly amended so that it has the flexibility to support a broader range of use cases beyond banking and energy, by making the accreditation model, technical standards and designation process less onerous.

---

4. 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 deliver privacy outcomes for individuals effectively and allow productive uses of data, while minimising compliance costs for businesses.

✳ While the Privacy Act provides flexibility overall, some requirements focus too much on specific controls (that is, prescribing certain actions or procedures) rather than outcomes. This contributes to excessive regulatory burden and costs to business without improving outcomes for individuals.

- For some regulated entities, the consent, notification and disclosure requirements in the Privacy Act are overly burdensome and difficult to comply with, 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.

✳ The Australian Government should amend the Privacy Act to embed an outcomes-based approach that enables regulated entities to fulfil their privacy obligations by meeting criteria that are targeted at outcomes, rather than controls-based rules.

✳ This should be achieved by introducing an overarching privacy duty for regulated entities to deal with personal information in a manner that is fair and reasonable in the circumstances. The Australian Privacy Principles should be phased out.

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 these 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 4.1). 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. The goal is to ensure that 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 4.1 – 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 chapter.

In Australia, the main legislation for protecting information privacy is the *Privacy Act 1988* (Cth) (box 4.2). 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 Act also recognises the need to balance the competing interests of regulated entities. Accordingly, one object of the Act is 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 object 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.

The Privacy Act in a changing data landscape

Since the Privacy Act was introduced, 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)

Box 4.2 – How does the Privacy Act work and who is covered?

The Privacy Act governs how personal information is handled. Section 6 defines personal information 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'.[a]

Responsibilities under the Privacy Act apply to most organisations with an annual turnover greater than $3 million and to 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 generally 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 individuals with access to their personal information upon request, unless an exception applies.

a. There is a proposal to amend the definition of 'personal information' (appendix F).

Today 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 2024c). 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. The resulting *Privacy Act Review* delivered its final report in 2023, and some of its recommended reforms were passed in late 2024 (appendix F).

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 2020a; Ai Group 2020; ICA 2020).

But this view was far from universal. Some inquiry participants saw the Act as overly burdensome and ineffective. The Productivity Commission's analysis demonstrates it can also be costly (box 4.3). As one participant in this inquiry 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)

> ## Box 4.3 – The cost of protecting privacy
>
> 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[a] (worth $13 billion per year). Regulation can also stifle 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 Productivity Commission heard that large organisations often have a central privacy team that conducts 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.
>
> More detailed information on data sources and assumptions is available in appendix B.
>
> **a.** Data use is determined by many factors, changes related only to privacy are unlikely to capture all potential benefits.

Another inquiry participant said:

> the Commonwealth's current Privacy Act, and the culture it has established within the bureaucracy towards data sharing – even across agencies and governments – has a meaningful impact on the quality of service delivery and expenditure of revenue that could otherwise be achieved. From a government-to-government data sharing proposition, the Privacy Act provisions significantly hamper data sharing within and between governments, limiting the impact their programs and services can have. (Tahnya Donaghy, sub. 76, p. 7)

There was a common view that the emphasis on consent, notification and disclosure is difficult to comply with, especially in the digital age. For example, Advanced Pharmacy Australia, representing hospital pharmacists nationally, told this inquiry:

> we support outcomes-based compliance approaches to privacy. Rigid controls-based rules often delay the safe implementation of pharmacy informatics projects without improving patient protection. (sub. 513, p. 8)

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)

Adobe 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' (2020, pp. 5, 9).

One inquiry participant said that the Act places 'excessive reliance' on 'form over substance' disclosures that do not 'promote good transparency' or encourage 'trustworthy data practices' (Peter Leonard, sub. 183, pp. 2, 3).

These views show that, while some regulated entities found the Act to be sufficiently flexible, some aspects of the regulatory regime were considered to focus too much on controls rather than outcomes (box 4.4).

- 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 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 and this inquiry, several business participants called for both greater certainty (including through more prescriptive rules) and greater flexibility in the Privacy Act regime.

In 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 not have 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 the requirement to have privacy policies, does 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)

Box 4.4 – 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 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 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 regulations. 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. In the context of the Privacy Act, the requirement in APP 1 to have a privacy policy is relatively flexible, as the policy can contain whatever the regulated entity considers appropriate. But the underlying privacy outcome is about aligning how personal information is treated with what individuals expect or are informed of – and APP 1 prescribes the procedure through which this outcome is to be achieved.
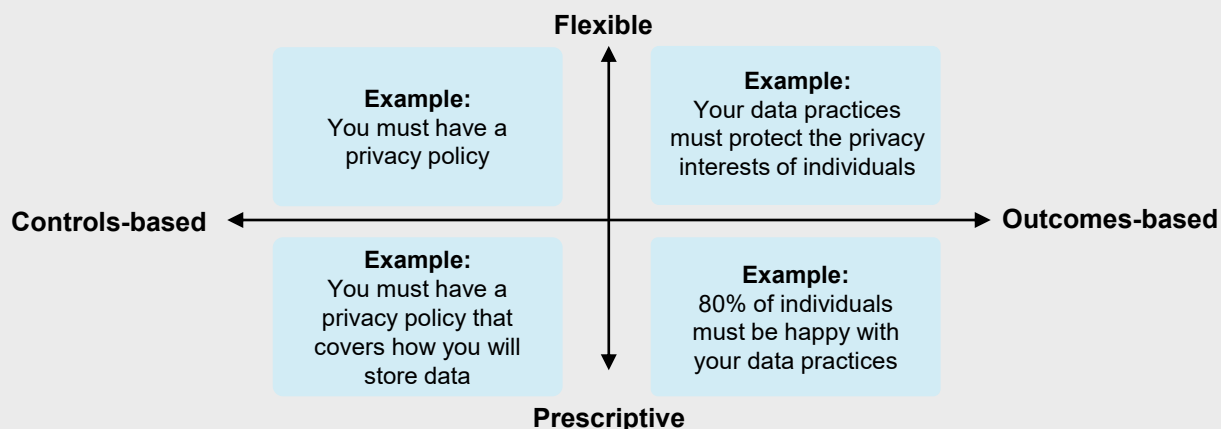
But many consider that 'privacy self-management' does not achieve the goals of the Privacy Act. Based on a nationally representative survey of 1,000 Australians, the Consumer Policy Research Centre found that 'only 7% of consumers agree that companies give consumers real choices to protect their privacy online', with '52% of consumers finding it time-consuming to protect their privacy online' (Gupta 2023b, p. 10).

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 requirement 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 long 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 use (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 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** are 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'[31] (CHOICE 2020, p. 4).

In response to the interim report, one participant stated that 'affected individuals, however diligent, are often not able to ascertain' whether the 'value exchange' of service for their consent is 'reasonable' (Peter Leonard, sub. 183, p. 8).

Similarly, the Consumer Policy Research Centre said that the reliance on notification and consent results in consumers being frequently forced into situations 'where they "decide once" about whether to share their data but bear the consequences potentially for the remainder of their life … [which is] … not a fair trade' (CPRC, sub. 594, p. 4).

The Australian Retailers Association & National Retail Association told this inquiry that current controls-based requirements 'often create "consent fatigue", where individuals are presented with so much information that they disengage entirely' (sub. 533, p. 6).

---

[31] 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).

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)

A positively framed regulatory framework could reduce the burden on individuals who currently struggle to constantly 'make informed and rational decisions with little market intervention' to protect themselves from harm (Gupta 2023a, p. 4).

Renewing the focus on privacy outcomes

As discussed, regulation that focusses too heavily on controls, as opposed to outcomes, can dampen innovation. This is because even if the actions or procedures required by the regulation seem individually 'sensible', they may not be the only, let alone the most efficient or effective, way to meet the regulatory objective. Under a controls-based regime there is limited ability for regulated entities to find new – and potentially more innovative – 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 for individuals – rather, it is about achieving those privacy objectives in a more flexible and effective manner.

An outcomes-based privacy duty embedded in the Privacy Act

The primary 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 outcomes-based approach 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 4.5). These could be adapted to create a similar duty or obligation (that is, a legal requirement that governs how a person acts or behaves) in relation to privacy.

The PC considers that introducing an overarching **outcomes-based privacy duty** that is embedded in the Privacy Act is the best way to achieve the objectives of privacy regulation, in a world where the nature of business models and data uses are changing rapidly as technology evolves. This option would reorient Australia's privacy regime, as a whole, towards outcomes-based requirements and could ultimately replace many existing controls-based requirements in the Privacy Act.

An outcomes-based privacy duty would operate both proactively and reactively. It would apply irrespective of consent to effectively shift responsibility for protecting personal information clearly onto regulated entities. It would raise the bar and create a clear baseline expectation of privacy protection for personal information by all regulated entities in Australia. To illustrate, figure 4.1 provides a worked example of actions that may fulfil the privacy duty both before and after a data breach.

Box 4.5 – Examples of duties and obligations

- In financial services, **best interest obligations** require some types of service providers to prioritise and act in the best interests of their client. This includes financial advisers (under the *Corporations Act 2001* (Cth), Part 7.7A) and mortgage brokers (under the *National Consumer Credit Protection Act 2009* (Cth), Part 3-5A). These obligations are framed as high-level principles and outcomes, for example, in the case of mortgage brokers, 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 2023b, p. 10).

Figure 4.1 – Actions that may fulfil the privacy duty in the context of a data breach

Scenario: a data breach

What actions could a company take to fulfil the privacy duty – both proactively and reactively – when personal information about customers is stolen causing a data breach?

Examples of proactive actions (ex ante)	Examples of reactive actions (ex post)
• Considered decisions and transparency about what data is being collected and why • Robust security such as encryption, firewalls and secure authentication • Risk assessments to identify vulnerabilities in systems and processes with appropriate controls put in place • Staff training on data protection, phishing risks, and safe handling of personal information • Controlled data access – limited to staff whose roles specifically require the data • Data breach response plan developed and tested	• Notify affected individuals providing information on the breach and potential risks • Report to authorities as required by law (OAIC) • Damage mitigation to contain the breach, recover lost data and prevent further unauthorised access • Offer support to impacted customers • Restore systems and secure operations • Critically review breach event to identify causes and update policies and technical controls to prevent any similar event in the future

This scenario is illustrative of actions that may be sufficient to meet the relevant duty.

The Australian Retailers Association & National Retail Association submitted to this inquiry:

a shift to outcomes-based obligations … would better protect consumers while allowing businesses to provide clear, meaningful information without excessive red tape (sub. 533, p. 6).

The creation of an outcomes-based duty could also alleviate the incidence of overcompliance (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 the privacy duty without them. A privacy duty 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).

What could an outcomes-based privacy duty look like?

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 Act to accommodate different business models (ARCA 2020, p. 6; Google 2020, p. 2; Guardian Australia 2020, p. 5; IGEA 2020, p. 6). 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 & 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, 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. (qr. 45, p. 2)

To enable this, the PC recommends an overarching privacy duty based on the adaptable and scalable legal principles of **fairness and reasonableness** in the circumstances. The interim report canvassed several options for how an outcomes-based obligation could be framed, including:

- a best interest obligation, which would require regulated entities to act in the best interest of an individual in respect of their privacy
- an obligation for regulated entities to have regard to the best interest of an individual in respect of their privacy – this would require the regulated entity, when making decisions about how to act, to consider the privacy interests of individuals, but not necessarily prioritise those interests
- a duty of care, which would require regulated entities to take steps to prevent reasonably foreseeable harm to an individual's privacy.

The interim report also discussed whether outcomes-based obligations should be implemented in the Privacy Act as an overarching framework or as an alternative (dual track) compliance mechanism. The PC recommends that outcomes-based obligations should be implemented as an overarching framework because, as some participants argued, multiple compliance pathways could create additional complexity and make compliance and enforcement difficult (AGD, sub. 602, p. 4; CSIRO, sub. 322, p. 8).

Why fair and reasonable?

After extensive consultation, the PC considers that a 'fair and reasonable in the circumstances' standard is most appropriate for an overarching privacy duty. Submissions to this inquiry expressed clear support for a fair and reasonable standard to be applied as an overarching threshold for privacy regulation in Australia.[32]

The Office of the Australian Information Commissioner (OAIC) has previously said that 'fairness and reasonableness have always been key concepts underlying the protections in the Privacy Act' and that reasonableness is a 'widely understood legal threshold' (2020, p. 84). There are also links to adjacent areas of law.

> Fairness and reasonableness are important concepts in both the Privacy Act and the [Australian Consumer Law], and the OAIC anticipates that APP entities will be able to be guided by existing precedents on these principles. (2020, p. 88)

In its submission, the Attorney-General's Department said that 'fairness and reasonableness are widely recognised concepts in Australian law (including anti-discrimination, employment and consumer law)' (sub. 602, p. 4). Another submitter said:

> concepts of reasonableness underpin many statutes and the common law, including the tortious duties of care that all legal entities are expected to understand, interpret and apply every day in and to all of their activities. (Peter Leonard, sub. 100, p. 10)

In response to the interim report, a 'fair and reasonable in the circumstances' standard for privacy was supported by a range of participants (ADM+S, sub. 412, pp. 20–21; Kemp et al., sub. 449, p. 3; Law Council of Australia, sub. 599, p. 22).

Importantly, the PC's recommendation in this report differs from the proposal in the Privacy Act Review to integrate a 'fair and reasonable' test within some of the existing APPs – as in the PC's view that proposal would impose *additional* requirements on the collection, use and disclosure of information (AGD 2023b, pp. 120–121) together with the full suite of existing controls-based regulation; whereas this recommendation is about creating new outcomes-based requirements *instead of* controls-based regulation.

Reducing complexity and cumulative regulatory burden is key to enabling productivity and innovation. The PC heard that in discussions of privacy reform:

> There is a temptation to keep adding layers to the cake of regulatory obligations … It is appropriate to push back against that temptation. Data privacy rules need to be right-sized and fit for purpose. (Peter Leonard, sub. 100, p. 1)

Regimes that combine an overarching legislative duty with supporting codes of practice and/or guidance outside of legislation already exist in several other regulatory areas, such as work health and safety and the United Kingdom's consumer duty (box 4.6).

---

[32] It should be noted that these comments were made in the general context of the 'fair and reasonable' standard being introduced in addition to the APPs.

Box 4.6 – Outcomes-based obligations supported by codes and regulatory guidance

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

- **Outcomes-based compliance** – a person conducting a business or undertaking has a duty 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, 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 that 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). This allows entities to choose the safest and most efficient compliance pathways, resulting in greater innovation (for example, new safety technologies and flexible risk-management systems) while maintaining worker protection.

The Consumer Duty (United Kingdom)

- **Outcomes-based duty** – sets the standard of care that firms should give to customers in retail financial markets and applies flexibly and dynamically to new products, services and business models as they emerge. The consumer duty is interpreted in light of what is reasonable given the circumstances. All firms have the same responsibility to act to deliver good outcomes for retail customers, but the capabilities of a firm will differ depending on its size and activities (FCA 2022, pp. 3–4).
- **Regulatory guidance** – Finalised Financial Conduct Authority guidance provides detail on what the duty looks like in practice and how firms should comply with their obligations (FCA 2022). The framing gives firms autonomy to choose how to meet outcomes encouraging new designs and technology. Financial Conduct Authority guidance and supervision under the Duty emphasise proportionality and role-based responsibilities across the distribution chain. This reduces one-size-fits-all compliance, making it easier for smaller or innovative firms to participate, scale and boost productivity.

Implementing an outcomes-based privacy duty

Factors for consideration

An overarching privacy duty to deal with personal information in a manner that is fair and reasonable in the circumstances would clearly locate responsibility for data protection on data holders – while at the same time allowing for localised implementation and flexibility to promote innovation and bolster productivity.

To guide implementation, the privacy duty should be further scaffolded in the Privacy Act by principles-based factors for consideration (non-exhaustive to avoid recreating existing controls by another name) including transparency, proportionality and necessity. The use of common and well-understood **legal principles** to help inform the operation of the duty by regulators, judges, and regulated entities further allows for flexibility, scalability and tech-neutrality.

The factors for consideration would be of value particularly as the body of case law emerges, and to assist government in providing further guidance and support materials to operationalise the duty. Further detail on the proposed factors for consideration can be found in table 4.1.

Table 4.1 – Factors for consideration

	Description	Example
Proportionality	Generally framed around a *balancing* of interests between the actual benefit obtained against the specific burden imposed – that is, was the outcome for the regulated entity proportionate to the privacy impacts on the individual?	• What is the cost of implementing privacy protections? • What are the privacy risks to the personal information? • What are the benefits of the personal information to the regulated entity? • Are there less privacy-intrusive means available to achieve a similar outcome?
Necessity	Considers how the dealing with personal information is necessary to the functions and activities of the regulated entity	• Does the regulated entity need to deal with the personal information in this way to fulfil their functions and activities? • Is the dealing with personal information directly related to the regulated entity's stated purpose?
Transparency	How the individual has been provided with clear, current and understandable advice about the dealing with their personal information	• Where is the advice located? • Have crucial facts been buried in lengthy documents? • Is advice comprehensive and inclusive of all key facts? • Is the language used clear, and the advice provided simple and easy to understand?

These legal principles are featured in privacy regimes around the world. Principles of fairness and transparency are enshrined in the European Union's General Data Protection Regulation (GDPR) (Article 5.1.a). The principle of necessity is also a central element to the European Union's conditions for the lawful processing of data (GDPR, EU, Article 6.1) and the principle of proportionality frames what are considered to be 'legitimate interests' (GDPR, EU, Article 6.1.f). The principle of reasonableness also applies as an overarching standard in Canada's privacy regime for private regulated entities (Personal Information Protection and Electronic Documents Act 2000, Canada, c. 5, s. 5(3)).

In determining what is fair and reasonable in the circumstances it may also be appropriate to consider additional factors such as *individual interests* and the *public interest*.

The role of the regulator – to help business and consumers make the transition

Under the adoption of a general duty the existing Australian Privacy Principles would ultimately be phased out with a suggested **three-year transition period** as supporting documentation and other implementation tools are developed.

Practical implementation of the duty should be further assisted through comprehensive supporting documentation such as regulatory guidance, industry codes, templates and guidelines. Figure 4.2 shows the legislative and non-legislative components of the overarching outcomes-based privacy duty.

How should enforcement occur?

At present, enforcement of the Privacy Act is a key function of the regulator, the OAIC.

One participant in this inquiry said:

> for regulators, outcome-based approaches would enable more effective enforcement by allowing resources to be targeted on cases where privacy harm actually occurs, rather than procedural violations that may have minimal impact on individual privacy. (Skyscanner, sub. 197, p. 1)

Figure 4.2 – The overarching privacy duty

Privacy Duty – Fair and Reasonable in the circumstances (Privacy Act)			
Factors for consideration (Privacy Act)			
Transparency	Necessity		Proportionality
Implementation tools			
Templates	Regulatory guidance	Industry codes	Guidelines
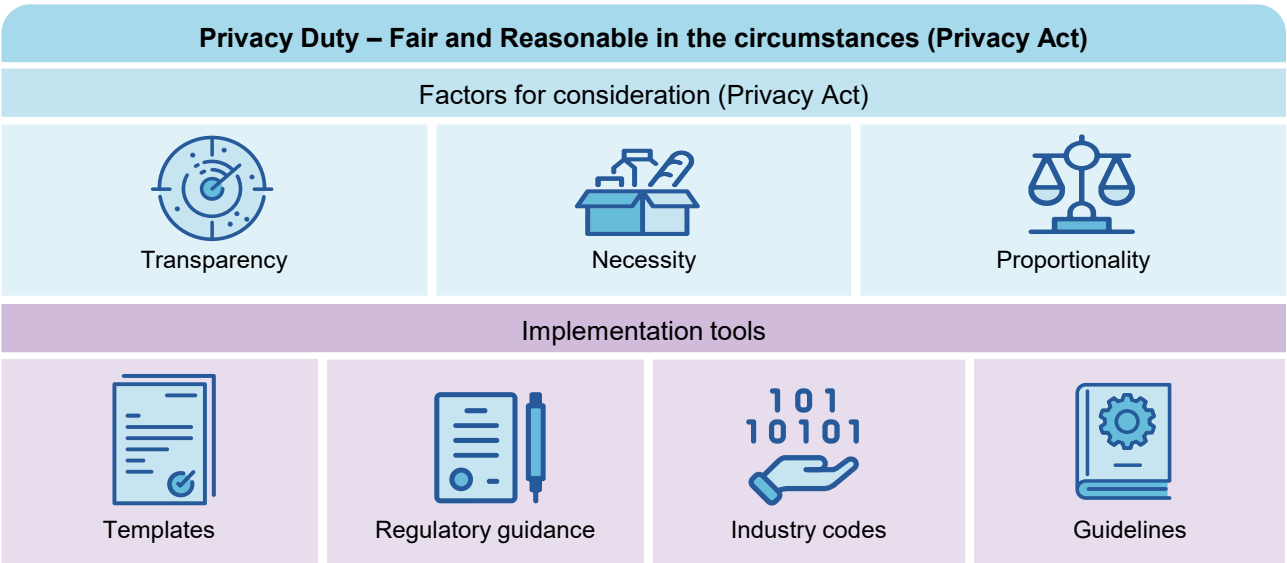
A key issue is the capacity and capabilities of the OAIC to undertake enforcement actions – and whether additional resourcing or regulatory architecture is needed to enable effective regulatory activity. The importance of sufficient resourcing is particularly acute given the shared expectation that the 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. (ICA, 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 and the establishment of a Deputy Commissioner for Enforcement (AGD 2023b, pp. 265–271).

There could be further 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). Such 'super complaints' can only be made by designated peak bodies who are allowed to make complaints concerning significant or systemic issues. The ACCC has 90 days to publicly respond and must publicly outline next steps (ACCC 2024b).

Another mechanism could involve the OAIC being specifically resourced to undertake test cases and develop a test case program. Over time, this would enhance regulatory certainty for the regulated entities, individuals and the regulator. This could mirror the test case litigation program operated by the Australian Taxation Office (ATO 2025).

» **Recommendation 4.1**
An outcomes-based privacy duty embedded in the Privacy Act

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

This should be achieved by introducing an overarching privacy duty for regulated entities to deal with personal information in a manner that is fair and reasonable in the circumstances.

The Privacy Act should be further amended to outline several non-exhaustive factors for consideration to guide decision-makers in determining what is fair and reasonable – including proportionality, necessity, and transparency. The existing Australian Privacy Principles should ultimately be phased out.

Implementation of the duty should be supported through non-legislative means including documentation such as regulatory guidance, sector-specific codes, templates, and guidelines.

The Office of the Australian Information Commissioner should be appropriately resourced to support the transition to an outcomes-based privacy duty.

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

Summary

✴ **Digital financial reporting has the potential to make the preparation, extraction and analysis of data in financial reports more efficient, transparent and accurate.**

- Investors, analysts and other report users could process financial information more efficiently, and auditors would be able to detect anomalies and emerging financial issues earlier. Regulators could undertake more effective risk targeting, while report preparers may benefit from improved global capital market visibility.

✴ **These benefits have not materialised in Australia, as no digital financial reports have been submitted, despite the fact that it has been 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 Australia is unlikely to realise the benefits of digital financial reporting under the existing voluntary scheme, since there is minimal value in a single report preparer voluntarily producing a digital report when no other preparers have chosen to.
- Artificial intelligence and other digital technologies provide a complement to, not a substitute for, digital financial reporting; to work effectively, these tools need the structure of a digital financial reporting taxonomy.
- While short-term transition costs present a barrier to the voluntary adoption of digital financial reporting, the available evidence suggests that costs fall over time and, for Australian report preparers, would be lower than the costs of non-digital report preparation in the long run.

✴ **The Productivity Commission recommends that half-yearly and annual digital financial reporting be mandated for disclosing entities as defined in the _Corporations Act 2001_ (Cth), which encompasses publicly listed companies and other public interest entities. The requirement for financial reports to be submitted in hard copy or PDF form should also be removed for these entities.**

- The Australian Securities and Investments Commission (ASIC) should set requirements for report preparation and, in conjunction with stock market operators, determine where and how reports are submitted.
- ASIC should also implement measures to ensure that reports contain high-quality financial data.
- Reports should be publicly and freely available, and easily downloadable.

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 large, high-income economies where it is mandatory to submit financial reports in a non-digital form, such as in hard copy or as a PDF file. The option to voluntarily submit digital financial reports has been available in Australia since 2010, but as of June 2025, no digital financial reports have been submitted (ASIC, sub. 2, p. 1). 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 form 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 generate some transition costs for report preparers and users, but ultimately 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 applies mostly 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 comply with the law. For some entities, such as **reporting entities** and **disclosing entities**, this includes a requirement to prepare financial reports (box 5.1). The Australian Securities and Investments Commission (ASIC) oversees compliance with the Act (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 5.1). Financial reports can be prepared in a non-digital form (for example, hard copy, PDF file or HTML file) or a digital form.

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. By contrast, **digital** financial reports are prepared in a form that is more efficient for data extraction and analysis, while also having the capacity to be as readable as non-digital reports. 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 5.2).

As well as traditional financial reports, requirements for some Australian entities to lodge sustainability reports began being phased in from 1 January 2025 (ASIC 2025e). The Australian Sustainability Reporting Standards require entities to 'disclose information about climate-related risks and opportunities that could reasonably be expected to affect [an] 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 form (ASIC, personal communication, 18 July 2025).

Box 5.1 – 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. Different entities have different reporting requirements.

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 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. 292). They are subject to a certain level of public interest and therefore have enhanced disclosure requirements, including a requirement to submit half-yearly financial 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, companies listed on the Australian Securities Exchange (ASX) 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.

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 2018a). **c.** For example, small proprietary companies must prepare financial reports if they are foreign-controlled.

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 5.2 – 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 than it is with 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 (in eXtensible Business Reporting Language (XBRL) format), 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

The benefits of digital financial reporting could be wide-reaching and substantial (figure 5.1).[33]

Deloitte Access Economics has estimated that introducing a digital financial reporting mandate could add $7.7 billion per year to the Australian economy after five years (2023, p. 13).[34] They estimated this figure on the basis that the mandate would apply to all businesses with over $50 million in annual revenue (one of three thresholds that defines a 'large company', with large companies needing to meet two of these three thresholds) (box 5.1; Deloitte Access Economics 2023, p. 28).

---

[33] Throughout the chapter, costs and benefits are assumed to apply broadly to report preparers or users, unless they are identified as applying to a smaller cohort – for example, publicly listed companies.

[34] A digital financial reporting mandate was estimated to cause short-term net costs to the economy while report preparers and users transitioned to the new requirements. Five years after the introduction of a mandate, the estimated ongoing mean annual net benefit rose to $7.7 billion (Deloitte Access Economics 2023, p. 14).

Figure 5.1 – The benefits of digital financial reporting would accrue to multiple parties

	Improvements to existing activities	Enabling of new activities
Report preparers	Improved information processing	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)	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 can be done more efficiently and accurately

Information in digital, machine-readable financial reports can be processed more efficiently and accurately (box 5.2). This increases productivity by both saving workers' time and improving the quality of their work (PC 2023c, p. 5).

For example, it is easier for **auditors** to extract and transform data from digital financial reports, giving them more time for analysis (Perdana et al. 2015, p. 125). And with increased access to digital financial information, auditors can '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**. Data aggregators working with *non-digital* reports must manually map line items from financial statements to their internal data taxonomy. For example, one data aggregator found that report preparers were using many different labels to describe a single item in a digital financial reporting taxonomy: the item *</CostofGoodsSold>* (in eXtensible Business Report language (XBRL) format) had been labelled, among other things, as 'Cost of Good Sold', 'Cost of goods sold', 'Cost of fuel sold' and 'Cost of goods sold and occupancy costs' (XBRL International 2013).

By comparison, the information within *digital* reports has already been assigned meaning from the 'tags' of a digital reporting taxonomy (box 5.2). In the case of the reports above, the uniquely labelled line items would already be consistently tagged as *</CostofGoodsSold>*, allowing aggregators to map data that has been prepared under one taxonomy to their internal taxonomy. This means that data can be extracted from financial reports more quickly and accurately.

When Taiwan transitioned from non-digital to digital financial reporting in 2012, one data aggregator saw at least a fourfold decrease in its report processing time, from about eight minutes per report to between one and two minutes (XBRL International 2013). Taiwan was also transitioning from non-digital *HTML* reporting to digital XBRL reporting. Extracting data from non-digital *PDF* reports – which are used in Australia – can take up to five times longer than extracting data from HTML reports (XBRL International 2013). Consequently, the time savings from a transition between PDF and digital XBRL reporting in Australia could be larger than what was observed in Taiwan.

Studies show mixed results on whether mandatory digital financial reporting reduces investors' information processing costs. 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 a narrowing of the information gap between small and large investors, suggesting that small investors' information processing costs had declined. 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 maintained that mandatory digital financial reporting had improved communication of financial information between listed firms and capital market participants.

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 is consistent with views shared by inquiry participants (box 5.3).

Box 5.3 – 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 … digital … this would save time and effort, and increase the quality of research. (David Hardidge, qr. 19, pp. 2–3)

Structured digital reports allow easier access to comparable financial data across companies and time periods. This improves market transparency and strengthens investor oversight. (ASA, sub. 44, p. 1)

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. Digital [reports] would allow for easier comparison and analysis. (ADHA, 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 adoption of digital financial reporting may seem peripheral to transport at first glance, but for publicly listed mobility firms, infrastructure investors, and [electric vehicle] fleet operators, it could improve transparency, reduce compliance costs, and attract capital for large-scale decarbonisation and automation projects. (ITS Australia, sub. 428, p. 3)

Government agencies are also confident they would benefit from greater uptake of digital financial reporting. ASIC stated 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 to more effectively evaluate the potential impact of changes to accounting standards.

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. (AASB 2019, p. 13)

Evidence from taxation reporting suggests that a shift to digital reporting can create sizeable benefits. The Australian Taxation Office estimated that the 15 million digital reporting transactions made via their digital reporting-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 digital reporting for taxation purposes has continued to accelerate: 593 million and 1.3 billion 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).

Digital financial reporting could enable innovation

Digital financial reporting could enable a number of innovative practices seen overseas. Evidence from the United States suggests that **report users** are conducting 'big data' research and analysis with the large volumes of data generated by digital financial 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 its 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).

Australia risks being left further behind without adopting digital financial reporting. Australia's adoption of this technology already 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).[35] 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 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. (2024)

Similarly, Chartered Accountants Australia and New Zealand (CA ANZ) 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. (2025, p. 3)

---

[35] 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).

There is unmet demand for digital financial reports

Australian financial report users are keen to have greater access to digital financial reports. In CA ANZ's most recent survey of retail investors, about 70% of investors supported making digital financial reporting mandatory, while more than half said 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 also supported 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.[36]

Australia will not realise the benefits of digital financial reporting under a voluntary scheme

Upfront costs and market failures obstruct voluntary uptake

Australia is unlikely to realise the benefits of digital financial reporting if the existing voluntary submission scheme is maintained. The Productivity Commission 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 these costs have fallen over time for report preparers overseas, as box 5.4 outlines). In Australia, 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 form (ASIC 2025b)
- numerous other corporate, tax, business activity, governance and social responsibility reporting requirements (G100, sub. 1, pp. 4–6), with some, such as taxation reporting, completed digitally.

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

---

[36] 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.

Box 5.4 – International evidence indicates that the cost of preparing digital financial reports decreases as preparers gain experience

Before the introduction of mandatory digital financial reporting in the **United States**, the Securities and Exchange Commission (SEC) estimated the associated compliance costs for report preparers. In the first two years of the mandate, where preparers undertook simple block tagging[a] of footnotes in financial statements, the SEC estimated that costs would decrease by about 65% between preparers' first and subsequent submissions. Costs were also anticipated to fall by about 30% between preparers' first and subsequent submissions when detailed footnote tagging requirements were introduced in later years (PC calculations based on US SEC 2009, p. 133).

The SEC estimates appear to align with the actual costs borne by preparers: a 2018 study found that the average annual cost of preparing digital financial reports in the United States declined by 45% between 2014 and 2017 (AI CPA and XBRL International 2018, p. 1).

Similarly, in the **European Union**, a 2016 study by the European Securities and Markets Authority found that for report preparers outsourcing the tagging process, subsequent digital financial report submissions were expected to cost about 70% less than their first one. For report preparers producing digital financial reports in-house, subsequent submissions were estimated to be 65% cheaper (PC calculations based on ESMA 2016, pp. 64–65).

a. Block tagging is where segments of information are tagged as a single taxonomy item. Detailed tagging is where each disclosure item is assigned its own tag (David Hardidge, sub. 479, p. 2).

Digital financial reporting may also create **intangible costs**. For example, report preparers may consider that publishing more structured financial data limits their ability to construct a narrative around their financial results. They may also be concerned about other entities being able to analyse their financial information more easily, particularly in competitive markets.[37]

These costs present a barrier to the uptake of digital financial reporting under a voluntary system because report preparers themselves may not anticipate receiving significant benefits from digital reporting, particularly in the short term. Instead, as discussed, 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**[38] associated with the transition to digital financial reporting. Specifically, one benefit 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 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)

---

[37] 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).

[38] Coordination failures occur where multiple parties could benefit from undertaking a particular action together, but they fail to do so (typically because unilateral action leaves a party worse off than doing nothing). The 'do nothing' status quo represents a relatively bad outcome for these parties, and for society more broadly.

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 digital financial reporting will ever be substantially adopted under the current voluntary regime. This is consistent with overseas experiences. In Canada, only 25 companies had submitted a digital financial report after more than a decade of it being possible to do so, while the United States and South Africa both introduced mandatory digital financial reporting after seeing minimal uptake from voluntary schemes (Chen 2010, p. 24; Debreceny et al. 2012, p. 51; South African CIPC 2024; Troshani and Rowbottom 2022, p. 7).

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 common 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).

Technologies such as AI are a complement, not a substitute

The rapidly developing capabilities of artificial intelligence (AI) and other digital technologies raises the possibility that they are adequate substitutes for digital financial reporting (NAB, sub. 581, p. 21; Property Council of Australia, qr. 64, p. 3). 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. Without the underlying structure of a digital financial reporting taxonomy, AI tools like existing general purpose large language models (LLMs) are constrained in their capacity to predictably produce accurate analysis of unstructured data that has been extracted from non-digital financial reports.

When analysing non-digital components of financial reports from the United States, the best-performing LLMs extracted data with an accuracy rate of about 70%, but mapped financial items to the correct item in a financial reporting taxonomy at less than 20% accuracy (Wang et al. 2025, pp. 7–8).[39] By contrast, when digital financial reports are prepared, the financial data is tagged and structured within a consistent taxonomy (box 5.2), ready to be analysed using AI tools.

Inquiry participants saw potential in using digital financial reports and technologies such as AI in a complementary way (box 5.5), and many inquiry participants recognised the need for AI tools to be underpinned by high-quality data.[40]

---

[39] 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. 14).

[40] ATN Universities, qr. 13, p. 3; AIIA, 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 5.5 – Inquiry participants see AI as a powerful complement to digital financial reporting, not a substitute

One of the main implementation issues [for digital financial reporting] is the use of unnecessary extensions – i.e., a suitable tag already exists in the taxonomy. Hopefully, with recent developments in AI, the various software tools have been, or are being updated, for the use of AI to identify already existing tags. (David Hardidge, sub. 479, p. 4)

High-quality digital reporting will … support the responsible use of emerging technologies, including artificial intelligence, which is increasingly used by both institutional and retail investors to interpret disclosures. (ASA, sub. 343, 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 … 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

It is hard to find data comparing the equivalent long-term cost of digital financial reporting with hard copy or PDF reporting, but there is some evidence for Australia to suggest that over the longer term, the annual cost of digital reporting could be as much as 40% lower.[41]

This estimate is driven by the fact that the cost of digital financial reporting falls as preparers gain experience with the process. 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 (lower than the $42,100 annual cost of producing *non-digital* financial reports estimated by Treasury) (2023, p. 29; 2018a).[42] Box 5.4 above also contains estimates that the costs of digital financial reporting in the United States and European Union have fallen or will fall over time.

Similarly, in the United States, Harris and Morsfield (2012, p. 23) observed these short-term cost and long-term benefit 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.

Another consideration is that financial reporting is a mandatory and well-established process. A digital financial reporting mandate would therefore represent a change in reporting form rather than an entirely new reporting requirement, as the underlying content that preparers are required to report would not change.

---

[41] Deloitte Access Economics estimated that an average large Australian company's ongoing annual cost of digital financial reporting would be $25,000 (in December 2022 dollars) (2023, pp. 29, 38), compared to the average annual cost of preparing and auditing *non-digital* financial reports for large companies, which the Treasury estimated to be $36,950 in mid-2019 ($42,100 in December 2022 dollars) (PC calculations based on ABS 2025d, table 7; Treasury 2018a). This equates to a saving of about 40%.

[42] 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 2018a).

Therefore, any consideration of the costs of digital financial reporting should focus where possible on the *additional* costs that preparers incur to produce financial reports in a digital form. One inquiry participant suggested that the costs associated with preparing reports in a digital form are small relative to the broader cost of financial reporting.

> A large, listed company typically spends over a thousand person-days preparing its annual report, alongside substantial external design and audit costs. Against this backdrop, the 3–10 person days required for tagging and review represent less than one percent of total effort [of preparing financial reports]. (XBRL International, sub. 260, p. 10)

Digital financial reporting should be the default

To capture the benefits of digital financial reporting, the PC recommends it be mandated. A mandate was endorsed by many inquiry participants providing feedback on the interim report.[43]

Some participants expressed conditional support for a mandate – for example, they raised the need for it to be accompanied by reporting relief for preparers, a cost-benefit analysis, the preservation of narratives around financial disclosures and data protection and cybersecurity measures.[44] Opportunities to address these concerns as part of implementing a digital financial reporting mandate are discussed below. Other participants suggested alternative approaches to a mandate, such as using AI to translate and structure data within and across financial reports, or incentives to promote voluntary uptake of digital financial reporting.[45]

A digital financial reporting mandate would give report preparers and users the certainty they need to invest in the infrastructure and processes that enable the productive use of digital financial reports, overcoming the coordination issues that were discussed above. As such, we are recommending mandatory digital financial reporting for disclosing entities as defined in the Corporations Act (recommendation 5.1). Implementing a digital financial reporting mandate will require consideration of the mandate's scope, as well as how reports are prepared, submitted and accessed (figure 5.2).

---

[43] ACTU, sub. 575, pp. 18–19; ASA, sub. 343, p. 1; ASCA, sub. 165, p. 2; ASX, sub. 438, p. 1; CA ANZ, sub. 560, p. 2; CoreFiling Limited, sub. 287, p. 4; CPA Australia, sub. 397, p. 4; EY Australia, sub. 418, p. 6; FinTech Australia, sub. 578, p. 4; KPMG Australia, sub. 349, p. 2; UWU, sub. 520, p. 23–24; XBRL International, sub. 260, p. 1.

[44] AICD, sub. 563, p. 3; BCA, sub. 488, p. 13; CME, sub. 386, p. 4; EFA, sub. 288, p. 12; G100, sub. 363, p. 5; Woolworths Group, sub. 596, p. 4.

[45] ACCI, sub. 424, p. 3; Consult Australia, sub. 373, p. 5; NAB, sub. 581, p. 21.

Figure 5.2 – Implementing a digital financial reporting mandate

Specifying the mandate's scope
The mandate should apply to annual and half-yearly **financial reports** prepared by **disclosing entities**. The Treasury should determine the thresholds for **phased implementation** of a mandate.

Setting requirements for report preparation
The existing **IFRS AU taxonomy** should be used. ASIC should continue to update the taxonomy annually. ASIC should specify **iXBRL** as the required format for digital financial reports.

Establishing the infrastructure and procedures for report submission
ASIC, along with market operators such as the ASX, should determine **where and how reports are submitted**.

Supporting the provision of high-quality, accessible digital financial data
ASIC should implement measures to ensure that digital financial reports contain **high-quality data**, such as: • establishing a data quality committee and/or industry advisory committee • integrating quality rules and validation checks into the submission process • setting guidelines around the use of taxonomy extensions. To enable users to harness the benefits of digital financial data, reports should be **publicly and freely available**, and **easily downloadable**.

Specifying the mandate's scope

The mandate should apply to disclosing entities ...

A digital financial reporting mandate should initially cover **disclosing entities** as defined in the Corporations Act. These include publicly listed companies and certain other public interest entities (box 5.1).

Some inquiry participants supported this scope (CA ANZ, sub. 560, p. 20; EY Australia, sub. 418, p. 6) or supported a potential phased transition to this scope, beginning with listed companies (CPA Australia, sub. 397, p. 4).

Participants indicated that the net benefits of digital financial reporting would be highest and most readily ascertained for this cohort – the pool of report users not only includes regulators and auditors, but analysts and investors too. The cost of transitioning to digital financial reporting is also expected to be relatively lower for disclosing entities: some are dual-listed companies that prepare digital financial reports in other jurisdictions, while others already use software that can prepare digital financial reports (CA ANZ 2025, pp. 18, 21; Workiva 2022).

Other inquiry participants suggested expanding the scope of a mandate to all reporting entities (box 5.1), either immediately or over time. Their reasons for expanding the scope included:

• transparency (CoreFiling Limited, sub. 287, pp. 4–5)

- because international evidence indicates that the benefits of digital financial reporting extend to all large entities (XBRL International, sub. 260, p. 3)
- because 'competitive fairness' should be maintained by subjecting similarly-sized listed and unlisted entities to the same reporting requirements (G100, sub. 363, p. 4).

On the latter point, because of their public interest nature, publicly listed companies are already subject to other enhanced reporting requirements relative to unlisted companies; these include continuous disclosure requirements and half-yearly financial reporting (box 5.1).

Inquiry participants also provided feedback on whether implementation of a digital financial reporting mandate should be phased. Several participants supported phasing,[46] with some suggesting specific schemes, such as a 12-month pilot followed by a 12-month limited mandate (G100, sub. 363, p. 4). Participants also identified that phasing would nurture feedback loops between stakeholders which can reduce the change impact on later adopters, enable smaller preparers to build technical maturity and reduce implementation risk by allowing the load on any new submission platform to grow incrementally. There was support for adopting a phased implementation approach starting with the largest entities (listed and unlisted), similar to the approach used for introducing mandatory climate-related financial disclosures (ASX, personal communication, 18 November 2025). However, another participant identified that phasing makes implementation more complex and temporarily fragments the information available to report users (CoreFiling Limited, sub. 287, p. 5).

In line with the introduction of other recent reporting mandates, such as sustainability reporting and Single Touch Payroll reporting (ASIC 2024; ATO 2021), the transition to mandatory digital financial reporting should be phased. As with mandatory sustainability reporting, the Treasury should determine the appropriate thresholds for phased implementation after consultation.

... and financial reporting

In the interim report, the PC sought feedback about whether a digital reporting mandate should be applied to other types of reporting, such as sustainability reporting. Some participants argued that a digital reporting mandate should cover sustainability reporting from the outset; otherwise, Australia's reporting requirements would not align with the 'global consensus' that sustainability reports are designed to be prepared digitally (XBRL International, sub. 260, p. 4). Participants also pointed to the limited marginal costs of extending a digital reporting mandate to sustainability reporting and the fact that 'communities, investors, and policymakers increasingly expect clear, consistent, and timely information on social and environmental performance, not just financial returns' (Seer Data & Analytics; sub. 408, p. 16; XBRL International, sub. 260, p. 4).

Other participants wanted an expansion to sustainability reporting to come later (ASA, sub. 343, p. 1; CA ANZ, sub. 560, pp. 20–21; EY Australia, sub. 418, p. 6). Some based this view on the Treasury's 2023 consultation on climate-related disclosures, which stated that the 'implementation of digital reporting for climate disclosure will not be pursued ahead of any plans to make digital reporting for existing financial reporting mandatory' (Treasury 2023c, p. 20). CA ANZ also noted that compared to digitising sustainability reporting, 'the need for reform is most acute in financial reporting … [digital financial reporting is] more feasible and urgently required' (sub. 560, p. 21).[47]

---

[46] AICD, sub. 563, p. 3; ASX, sub. 438, p. 2; BCA, sub. 488, p. 13; CA ANZ, sub. 560, p. 20.

[47] The PC notes that India is the only jurisdiction to have pursued mandatory digital sustainability reporting. Others, such as the European Union, have impending mandates (MSCI Institute 2025).

Given this, the initial scope of a digital reporting mandate should be half-yearly and annual **financial** reporting undertaken by disclosing entities. The legislative framework should accommodate the prospect of the mandate being expanded to cover other types of reporting – most notably, sustainability reporting.

Setting requirements for report preparation

Australia's digital financial reporting taxonomy is fit-for-purpose

The preparation of digital financial reports relies on the existence of a taxonomy: a data dictionary of definitions and terminology used in financial reporting. The Australian Government created a business-to-government digital reporting taxonomy (including for digital financial reporting) as part of the 2010 Standard Business Reporting reforms. 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, 114).

ASIC has updated 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 2025b).

Inquiry participants broadly agreed that the IFRS AU taxonomy is fit-for-purpose.[48] Working with this taxonomy would improve the global comparability of Australian financial reports and reduce compliance costs – for example, Australian entities already reporting digitally to the US SEC do so using the IFRS global taxonomy (US SEC 2024).[49] To ensure the IFRS AU taxonomy remains an appropriate standard in the future, ASIC's ongoing maintenance of the taxonomy could be conducted in consultation with an industry advisory committee, as discussed further below.

ASIC should specify iXBRL as the required format

Digital financial reports can be prepared in different formats, including as 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.[50] In **iXBRL** files, the digital financial information is interactively embedded in a document that can be read like a standard document, so the reports can be read by both humans and machines (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).

---

[48] ASA, sub. 343, p. 2; CA ANZ, sub. 560, p. 21; CoreFiling Limited, sub. 287, p. 5; EY Australia, sub. 418, p. 7; XBRL International, sub. 260, pp. 4–5. Another participant suggested adopting the IFRS taxonomy without any Australia-specific modifications (KPMG Australia, sub. 349, p. 2).

[49] Any taxonomy must also be consistent with Australian Accounting Standards. While those Standards do not prescribe that financial reports are prepared in any particular form (for example, non-digital or digital), 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.

[50] 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.

ASIC should be empowered to specify, from time to time, the format in which digital financial reports should be prepared. A number of inquiry participants expressed a preference for digital financial reports to be prepared in **iXBRL** format.[51]

If iXBRL were the required format for digital financial reports, **report preparers** would only need to prepare and submit a single document and could construct a narrative around their financial results, as they do with non-digital financial reports. This would go some way to addressing inquiry participants' concerns about preparers' reporting burden (BCA, sub. 488, p. 13; G100, sub. 363, p. 5; Woolworths Group, sub. 596, p. 4) and the need to ensure that 'qualitative business context' (for example, the narrative surrounding financial results) is not lost in digital financial reports (G100, sub. 363, p. 5).

iXBRL files also provide flexibility for **report users**. Users wishing to utilise both the digital and non-digital information from a financial report only need to review a single file. Those 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 disclosure review efficiency by the US SEC, the nation's corporate regulator. As part of the filing disclosure review process (which involves selective checks of company filings for compliance with accounting standards and other disclosure requirements) the SEC can issue comment letters, which are typically written feedback with requests for clarification. Wang et al. (2024, pp. 4–6) found that the US SEC was more likely to issue comment letters 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.

Given that the purpose of the SEC's disclosure review process – and comment letters – is to achieve high-quality public disclosure of financial information, efficient regulation facilitated by iXBRL filings not only benefits the regulator, but also the regulated report preparers – who can correct or improve information disclosure and avoid enforcement action – and report users via higher quality reporting.

Establishing infrastructure and procedures for report submission

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).[52]

Increased uptake from mandating digital financial reporting would require the implementation of a new lodgement mechanism. It will also need to be determined whether dual lodgement relief, where preparers that lodge financial reports with a market operator such as the Australian Securities Exchange (ASX) do not also need to lodge financial reports with ASIC, should be continued. [53]

Dual lodgement relief reduces the reporting burden experienced by publicly listed companies. It assists publicly listed companies to meet their continuous disclosure obligations and supports market integrity, with market operators able to facilitate timely, transparent and equal market access to disclosures of financial information

---

[51] ASA, sub. 343, p. 2; CA ANZ, sub. 560, pp. 21–22; CoreFiling Limited, sub. 287, p. 6; CPA Australia, sub. 397, p. 5; EY Australia, sub. 418, p. 7; NAB, sub. 581, p. 21–22; XBRL International, sub. 260, pp. 7–8.

[52] 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).

[53] There are four markets licensed to list securities in Australia: ASX, Cboe Australia, National Stock Exchange of Australia and Sydney Stock Exchange (ASIC 2025a).

(ASX, personal communication, 18 November 2025). However, establishing multiple submission platforms creates additional costs, and depending on how reports are made available to users after being submitted, increases the risk of financial information being disclosed to users in a fragmented or opaque way.

ASIC, together with market operators, should determine where and how digital financial reports are submitted. The arrangements should aim to minimise preparers' reporting burden while keeping reports accessible to report users, as discussed below.

Supporting the provision of high-quality, accessible data

ASIC should implement measures that enhance data quality

Realising the benefits of digital financial reporting depends on the value of reports to users. Appropriate regulatory requirements around reporting quality are crucial to ensure that **high-quality** financial data is prepared and submitted. Reports must also be **accessible** to users.

Australia's financial reporting legislative framework already contains regulatory requirements to ensure that submitted reports are of high quality. This includes requirements about the accuracy of data, audit processes and compliance with accounting standards (box 5.1). In response to the interim report, inquiry participants identified additional regulatory architecture that would promote the preparation and submission of high-quality digital financial data.

Broadly, inquiry participants highlighted the need to establish and maintain **feedback loops** between stakeholders (ASA, sub. 343, p. 2; CA ANZ, sub. 560, p. 21; XBRL International, sub. 260, p. 5), such as through the establishment of an industry advisory committee or a data quality committee as in the United States (ASX, sub. 438, p. 3). Ensuring that the experience of users is central to policy implementation and design is consistent with the stewardship approach identified in the PC's report on *Creating a dynamic and resilient economy* (2025b).

One potential area of oversight for a data quality committee would be **data quality rules** (ASX, sub. 438, p. 3).[54] Some data quality rules can be enforced 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). Inquiry participants supported similar checks being implemented in Australia (ASA, sub. 343, p. 2; CA ANZ, sub. 560, p. 21; David Hardidge, sub. 479, p. 3).

The steep decline in reporting errors since 2020 in the United States has been attributed to the creation and integration of data quality rules in report submission processes (Foshag 2025, p. 60; XBRL International, sub. 260, p. 5). Receiving warning messages when data quality rules are not being met in financial reports has improved preparers' capacity to detect and remediate errors before financial reports are submitted (Foshag 2025, pp. 10, 20).

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 makes it harder to compare financial reports (Perdana et al. 2015, p. 134). 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

---

[54] 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).

does appear to be becoming less common over time (Hoitash et al. 2020, pp. 116–117; UK FRC 2025). XBRL International (sub. 260, p. 6) proposed that Australia could take a similar approach to the European Union, where any extensions must be 'anchored' to an existing taxonomy concept. This approach would balance report preparers' need for flexibility and maintain some degree of comparability between reports.

Inquiry participants also shared views on the **assurance** of digital reports. Several supported incorporating digital reporting into assurance processes (ASA, sub. 343, p. 2; CA ANZ, sub. 560, p. 21). Participants also suggested making digital financial reports the official record of filing so that they are subject to governance and audit requirements (XBRL International, sub. 260, p. 4) and taxonomy audits to ensure financial reports comply with the digital financial reporting taxonomy (EY Australia, sub. 418, p. 7). While there is not yet a global consensus on best practice assurance of digital reports, inquiry participants noted that Australia should adopt international standards from the International Auditing and Assurance Standards Board when they become available (XBRL International, sub. 260, p. 7).

Implementing and maintaining many of these data quality measures will have cost implications for ASIC, and appropriate funding arrangements for this should be determined in consultation with the Treasury.

Reports should be publicly and freely available

To realise the benefits of digital financial reporting, the information within reports must be accessible to report users (CA ANZ 2025, p. 21). Accordingly, several inquiry participants said that digital financial reports should be publicly and freely available,[55] as well as easily downloadable (ASA, sub. 343, p. 2). Some participants also said that the platform holding digital reports should incorporate Application Programming Interfaces (APIs) (CA ANZ, sub. 560, p. 22; David Hardidge, sub. 479, p. 4; XBRL International, sub. 260, p. 10). APIs could enable automatic retrieval and bulk download of digital financial reports, making it easier for analysts, researchers and regulators to work with digital financial data at scale.

At present, financial reports are publicly available via ASIC for a fee (ASIC 2025c).[56] The Corporations (Fees) Regulations 2001 (Cth) (schedule 2, item 16) specify the fee that ASIC must charge for document access.[57] Providing a 'free access' portal, where costs are not directly recovered via search fees, is therefore not possible under current legislative arrangements.

One way to address this would be to amend the regulations to remove search fees associated with accessing financial reports, though this would have financial consequences for government. As with the data quality measures discussed above, the Treasury and ASIC should engage on how to address the cost implications that will arise from ensuring that digital financial reports are publicly and freely available.

Preparers' reporting burden should be reduced where possible

As discussed above, while financial reporting is a mandatory and well-established requirement for disclosing entities, the transition to preparing reports in a digital form will create costs.

Inquiry participants 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; G100, sub. 1, p. 3).

---

[55] ASA, sub. 343, p. 3; CA ANZ, sub. 560, p. 22; CPA Australia, sub. 397, p. 6; David Hardidge, sub. 479, p. 3; ICA, sub. 330, p. 6; XBRL International, sub. 260, p. 9.

[56] Some companies also publish financial reports on their website.

[57] Search fees are incurred where documents or copies of documents are provided on request. The fees were set when most services were paper-based and approximated the cost incurred to retrieve and provide the documents (Treasury 2018b, p. 13).

In addition, the requirement for financial reports to be submitted in hard copy or PDF form should be removed when mandatory digital financial reporting is implemented.

Preparers' reporting burden could also be reduced through:

- the use of AI tools when tagging financial reports (for example, to search for an appropriate tag from the taxonomy) (David Hardidge, sub. 479, p. 4)
- ASIC undertaking 'proportionate and pragmatic' supervision and enforcement in the early years of a digital financial reporting mandate, akin to their approach supporting the introduction of mandatory sustainability reporting in 2025 – for example, by providing entities with the opportunity to make changes to reports that have been identified as incorrect, incomplete or misleading in any way (ASIC 2025d, pp. 48–49)
- investigating opportunities for the re-use of digital financial data in other forms of business-to-government reporting – for example, using digital financial data submitted to ASIC to replace or supplement some questions in ABS surveys, such as the Quarterly Business Indicators Survey (ABS, sub. 587, p. 6).

» **Recommendation 5.1**
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 annual and half-yearly financial reporting mandatory for disclosing entities. The requirement for financial reports to be submitted in hard copy or PDF form should be removed for these entities. The implementation of mandatory digital financial reporting should be phased, with the Treasury determining the appropriate timelines for this approach.

Setting requirements for report preparation

The existing International Financial Reporting Standards (Australia) (IFRS AU) taxonomy should be used for digital financial reporting. The Australian Securities and Investments Commission (ASIC) should continue to update the taxonomy annually.

ASIC should be empowered to specify, from time to time, the format in which the reports must be prepared. At present, ASIC should specify inline eXtensible Business Reporting Language (iXBRL) as the required format.

Establishing infrastructure and procedures for report submission

ASIC, together with market operators such as the Australian Securities Exchange, should determine where and how digital financial reports are submitted. The arrangements should aim to minimise preparers' reporting burden while keeping reports accessible to report users.

Supporting the provision of high-quality, accessible digital financial data

ASIC should implement the measures necessary to ensure that digital financial reports contain high-quality data. ASIC could (among other actions):

- establish a data quality committee that would develop guidance and rules to improve data quality
- integrate automated validation checks into the submission process
- set guidelines around the use of taxonomy extensions and report format
- maintain feedback loops with stakeholders.

To enable report users to harness the benefits of digital financial data, digital financial reports should be publicly and freely available, and easily downloadable.

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. We held 193 meetings with 138 individual organisations (table A.1) and held three roundtables (table A.2). A consultation questionnaire was released on 19 May 2025 seeking feedback on specific aspects of our policy reform areas. The interim report was released on 5 August 2025, with feedback invited via a call for submissions. In total, 774 submissions (table A.3) and 75 questionnaire responses (table A.4) were received. Read submissions and questionnaire responses.

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

Table A.1 – Consultations

Participants
A New Approach (ANA)
Amazon AU
ARC Centre of Excellence for Automated Decision-Making and Society (ADM+S)
Ashurst
Associate Professor Katharine Kemp
Associate Professor Rita Matulionyte
Association for Data-driven Marketing & Advertising (ADMA)
Australasian Performing Right Association and Australasian Mechanical Copyright Owners Society (APRA AMCOS)
Australia New Zealand Screen Association (ANZSA)
Australian Agritech Association (AusAgritech)
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)

Participants

Australian Government Department of Finance (DoF)

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 (DITRDCSA)

Australian Government Office of the Arts (Indigenous Cultural and Intellectual Property)

Australian Government Treasury

Australian Information Industry Association (AIIA)

Australian Institute of Company Directors (AICD)

Australian Loyalty Association (ALA)

Australian Mobile Telecommunications Association (AMTA)

Australian Production Design Guild (APDG)

Australian Publishers Association (APA)

Australian Recording Industry Association (ARIA)

Australian Securities and Investments Commission (ASIC)

Australian Securities Exchange (ASX)

Australian Shareholders' Association (ASA)

Australian Society of Authors

Australian Taxation Office (ATO)

Australian Writers' Guild (AWG)

Bill Hero

Biza.io

Bureau of Communications, Arts and Regional Research (BCARR)

Bureau of Meteorology (BoM)

Business Council of Australia (BCA)

Challenge Networks

Chartered Accountants Australia and New Zealand (CA ANZ)

CHOICE

Cloudflare

Coles

Commonwealth Bank of Australia (CBA)

Commonwealth Scientific and Industrial Research Organisation (CSIRO)

Communications Alliance

Connected Farms

Participants

Participants
Consentic
Consumer Policy Research Centre (CPRC)
Copyright Advisory Group (CAG)
Copyright Agency
Creative Australia
Data Standards Body
Data Transfer Initiative (DTI)
Data61
Delia Rickard
Deloitte
Digital Industry Group Inc (DIGI)
Dr Bill Roberts
Dr Ian Oppermann
Dr Kylie Pappalardo
Dr Steve Lockey
Energy Flex
eSafety Commissioner
FinTech Australia
Fortinet
Glenn Cooper
Google Australia and New Zealand
GrainGrowers
Grocerize
Ground Up Privacy
Group of 100 (G100)
Helios Salinger
Hon Dr Andrew Leigh MP
Honorary Associate Professor Glenn Archer
Human Technology Institute (HTI)
HWLE Lawyers (Nicholas Pullen and Scott La Rocca)
IAB Australia (IAB)
Inrupt
Interactive Games & Entertainment Association (IGEA)
Jobs and Skills Australia (JSA)

Participants

KomplyAi

Long Street Advisors

Maincode

Mastercard (Australasia)

Media, Entertainment & Arts Alliance (MEAA)

Medical Software Industry Association (MSIA)

Meeco

Meta

Microsoft

Motion Picture Association Asia-Pacific

National Australia Bank (NAB)

National Farmers' Federation (NFF)

National Women's Alliances

Nordic Institute for Interoperability Solutions (NIIS)

Office of the Australian Information Commissioner (OAIC)

Office of the National Data Commissioner (ONDC)

Open Banking Limited

OpenAI

Optiver

Pairtree Intelligence

Peter Harris

Peter Leonard

Philip Coppel KC

Professor Dilan Thampapillai

Professor Isabella Alexander

Professor Jeannie Paterson

Professor Jill McKeough

Professor Joshua Gans

Professor Kathy Bowrey

Professor Kimberlee Weatherall

Professor Lauren Willis

Professor Leanne Wiseman

Professor Nicolas Suzor

Professor Nicole Gillespie

Participants

Participants
QBE Insurance Group
Quantium
Rigby Cooke Lawyers
Screen Producers Australia (SPA)
Solar Analytics
Sovereign Australia AI Pty Ltd
Tech Council of Australia (TCA)
Therapeutic Goods Administration (TGA)
United Kingdom Department of Business and Trade
Visa
Vocus
WeMoney
WiseList Pty Ltd (WiseList)
Woolworths Group
XBRL International, Inc (XBRL International)
Xero
Yahoo
Yamaha Agriculture Australia

Table A.2 – Roundtables

29 September 2025 – Farm machinery and equipment data roundtable

Participant	Organisation
Christina Blumberg	ACCC
Noah Tasker	AgriFutures Australia
Meg Lovegrove	Agritech Australia
Kristy Barber	Australian Farm Institute
Jake Sullivan	Australian Government Treasury
Dr David Lemon	CSIRO
Tess O'Hagan	Farmbot
David Lamb	Food Agility CRC
Professor Leanne Wiseman	Griffith Law School
Warwick Ragg	National Farmers' Federation
Zac Rayson	National Farmers' Federation
Charlotte Wundersitz	National Farmers' Federation
Hamish Munro	Pairtree Intelligence
Tim Gentle	Think Digital
Chris Mendes	Yamaha Agriculture Australia

30 September 2025 – Copyright roundtable

Participant	Organisation
Joseph Mitchell	Australian Council of Trade Unions
James Barton	Amazon Web Services
Rohini Sivakumar	Australian Recording Industry Association
Jock Given	Australian Society of Authors
Stuart Glover	Australian Publishers Association
James Lawrence	Copyright Society of Australia
Josephine Johnston	Copyright Agency
Rick Aarons	CSIRO
Bec Turner	Google Australia and New Zealand
Kate Haddock	Law Council of Australia, IP Committee
Associate Professor Rita Matulionyte	Macquarie University Law School
Fei Wu	Microsoft
Paul Davies	Media, Entertainment & Arts Alliance

30 September 2025 – Copyright roundtable

Participant	Organisation
James Dickinson	Screenrights
Calida Tang	Tech Council of Australia

1 October 2025 – Data access pathways roundtable

Participant	Organisation
Amanda Dadd	ACCC
Jill Berry	Adatree
Taylor Black	Australian Government Department of Finance
John Shepherd	Australian Government Department of Finance
Anna Nitschke	Australian Government Treasury
Miles Langford	Australian Retailers Association
Stuart Low	Biza.io
Peter Worthington-Eyre	Clearcore / AIHW
Erin Turner	Consumer Policy Research Centre
Dr Paul Tyler	Data61
Dr Ian Oppermann	Data Standards Body
Rob Finney	Intelematics
Cheng Lim	King & Wood Mallesons
Mitch Thorp	Mastercard (Australasia)
Katryna Dow	Meeco
Victor Bajanov	Quantium
Patrick Kennedy	Standards Australia

Table A.3 – Submissions

Participants	Sub no.
Acacia Calder McTainsh	704
Accenture	522
Adam Marsh	214
Adele Stevens	749
Adelina Tabila	90
Adobe	307
Advanced Pharmacy Australia (AdPha)	513
Aiden Umbrello	742
Aimee Lindorff	555
Ainsley Ewart	740
Airdrie Makim	576
AIUC Global Pty Ltd (AIUC Global)	600
Alako M	673
Alannah & Madeline Foundation	119
Alethux	561
Alex Adsett Literary	404
Alexander Swords	177
Alexandra McPaul	709
Aley Wild	662
Alicia Olive	708
Alison Bigg	463
Alison Stegert	156
Amanda Curtin	170
Amara Cavahlo	72
Amazon	535
Amazon AU	33
Anastasia Beasley	331
Anastasia Ferguson	494
ANDHealth	94
Andrea Innocent	414
Andrea Rowe	148
Andrew Fairclough	426
Andrew Paranavitana	671

Participants	Sub no.
Angela Collier	660
Angela O'Brien-Malone	182
Angus Lyttle	124
Anne Tedesco	611
Annette Braunack-Mayer	396
Anniemay Parker	153
Applause Genie	87
ARC Centre of Excellence for Automated Decision-Making and Society (ADM+S)	14, 412
ARC Centre of Excellence for the Digital Child (Digital Child)	379
Artelle Lenthall	447
Arts Law Centre of Australia (Arts Law)	490
Asher-Kyla Wood	635
Ashleigh Lawrence	83
Ashley Kalagian Blunt	139
Associate Professor Katharine Kemp, Professor Kathy Bowrey, Professor Mimi Zou, Associate Professor Daniel Joyce, Associate Professor Kayleen Manwaring, Dr Lucien J van Romburg, and Mr Anthony Ross	449
Association for Data-Driven Marketing & Advertising (ADMA)	46, 295
Association of American Publishers	501
Association of Artist Managers (AAM)	364
Attorney-General's Department (AGD)	602
Augusta Wendt	234
Ausfilm	528
Australasian Institute of Digital Health (AIDH)	516
Australasian Music Publishers' Association Limited (AMPAL)	319
Australasian Performing Right Association and Australasian Mechanical Copyright Owners Society (APRA AMCOS)	542
Australian Academy of Science (AAS)	38, 591
Australian Academy of Technological Sciences & Engineering (ATSE)	12
Australian Association of National Advertisers (AANA)	399
Australian Association of Voice Actors (AAVA)	264
Australian Automobile Association (AAA)	567
Australian Automotive Aftermarket Association (AAAA)	354
Australian Broadcasting Corporation (ABC)	350

Participants	Sub no.
Australian Bureau of Statistics (ABS)	587
Australian Catholic University (ACU)	515
Australian Chamber of Commerce and Industry (ACCI)	19, 424
Australian College of Nursing (ACN)	549
Australian Communications and Media Authority (ACMA)	498
Australian Communications Consumer Action Network (ACCAN)	37
Australian Competition and Consumer Commission (ACCC)	495
Australian Copyright Council (ACC)	485
Australian Council of Trade Unions (ACTU)	31, 575
Australian Digital Health Agency (ADHA)	505
Australian Digital Inclusion Alliance (ADIA)	163
Australian Film/TV Bodies	40, 541
Australian Finance Industry Association (AFIA)	565
Australian Financial Markets Association (AFMA)	27, 360
Australian Higher Education Industrial Association (AHEIA)	358
Australian Information Industry Association (AIIA)	4, 301
Australian Institute for Machine Learning (AIML)	60
Australian Institute of Company Directors (AICD)	18, 563
Australian Libraries and Archives Copyright Coalition (ALACC)	367
Australian Livestock and Rural Transporters Association (ALRTA)	556
Australian Medicines Handbook (AMH)	410
Australian National University, National Centre for the Public Awareness of Science (ANU)	566
Australian Psychological Society (APS)	558
Australian Publishers Association (APA)	523
Australian Recording Industry Association and Phonographic Performance Company of Australia (ARIA and PPCA)	489
Australian Research Data Commons (ARDC)	422
Australian Retail Credit Association (Arca)	366
Australian Retailers Association & National Retail Association (ARA & NRA)	21, 533
Australian Screen Industry Guilds (ASIG)	285
Australian Securities and Investments Commission (ASIC)	2
Australian Securities Exchange (ASX)	438

Participants	Sub no.
Australian Shareholders' Association (ASA)	44, 343
Australian Small Business and Family Enterprise Ombudsman (ASBFEO)	43, 583
Australian Smart Communities Association (ASCA)	165
Australian Society of Archivists	168
Australian Society of Authors	478
Australian Taxation Office	776
Australian Telecommunications Alliance (ATA)	317
Australian Writers' Guild and Australian Writers' Guild Authorship Collecting Society (AWG and AWGACS)	767
Authentic Design Alliance (ADA)	383
Ava Grace	679
AXiLe Informatics	568
Bailey Perkins	279
Barbara Temperton	572
Barnum Group Partnership	195
Benjamin Anderson	180
Benjamin Glover	711
Bernadette Jury	717
Beth Crighton	236
Beyond Blue	484
Billy Bright	721
Billy Temby	464
Blake M	145
BlueMere Books	106
Brandon Franklin	247
Bronwyn Saunders	184
Brooke Fuerste	286
Brotherhood of St Laurence (BSL)	308
Bryn Fenemor	741
Budjarn Lambeth	62
Bunnings Group	22
Business Council of Australia (BCA)	16, 488

Participants	Sub no.
Business Software Alliance (BSA)	337
Cadance Bell	361
Calabash Solutions	362
Callum Young	642
Campbell Border	199
Cara Tune	272
Carolyn Newson	217
Cassandra Hamer	93
Catherine Ward	731
Cecelia Ramsdale	152
Ceilidh Newbury	202
Centre for AI, Trust and Governance, University of Sydney	598
Centre for Artificial Intelligence and Digital Ethics, The University of Melbourne (CAIDE)	769
Cha Spencer	680
Chamber of Commerce and Industry Western Australia (CCIWA)	25
Chamber of Minerals and Energy WA (CME)	386
Char Najjar Photography	282
Charlotte Rose	374
Chartered Accountants Australia and New Zealand (CA ANZ)	560
Chelsea Davis	616
Cheryl Foong	115
Chic Management (Brisbane) Pty Ltd (Chic Brisbane)	394
Children's Cancer Institute (CCI)	126
Chris Ross	678
Chris Thrum	571
Christina Lacy	675
Cindy Aulby	614
Civil Contractors Federation Australia Ltd (CCF)	8
Coast Community News (CCN)	123
Coca-Cola System	17
Colin Griffith	512
Commonwealth Bank of Australia (CBA)	35
Commonwealth Scientific and Industrial Research Organisation (CSIRO)	322
Consult Australia	373

Participants	Sub no.
Consumer Healthcare Products Australia (CHP Australia)	762
Consumer Policy Research Centre (CPRC)	594
Copyright Advisory Group – Schools (CAG Schools)	517
Copyright Advisory Group – TAFE (CAG TAFE)	518
Copyright Agency	473
Copyright Alliance	502
CoreFiling Limited	287
Council for the Humanities, Arts and Social Sciences (CHASS)	333
Council of Small Business Organisations of Australia (COSBOA)	30, 524
CPA Australia	397
Creative Australia	432
Creative Commons, Creative Commons Australia, Wikimedia Australia	250
Creative Economy Pty Ltd (Creative Economy)	443
Curated Originality, TA Hart & Co (Hart & Co)	417
Curious About Ai	244
Dairy Australia	595
Dan McNamee	291
Dani Andrée	79
Danica Roberts	605
Daniel Aleksic	465
Daniel Gray-Barnett	582
Daniel Kjellin	191
Daniel Stacey	241
Daniel White	259
Daniel Witchey	618
Danielle Binks	203
Danielle Caruana	710
Danny Smith	200
Data Transfer Initiative (DTI)	194
Dave Kerr	127
David Follett	686
David Gould	284
David Hardidge	479
David Keegan	546

Participants	Sub no.
David Lee	89
David Martin	85
Deborah Abela	95
Deborah Pergolotti	584
Delilah Walsg	613
Diana Evans	211
Diane Finlay	50
Didirri Peters	49
Digital Economy Council of Australia (DECA)	15
Digital Health Cooperative Research Centre (DHCRC)	757
Digital Industry Group Inc (DIGI)	42, 759
Digital Platform Regulators Forum (DP-REG)	482
Digital Publishers Alliance (DPA)	384
Digital Rights Watch (DRW)	311
Dimity Powell	114
Dinuka McKenzie	84
Docusign	348
Dongheyon Kim	138
Dr Lyndall Bryant et al	536
Electronic Frontiers Australia Inc (EFA)	288
Elizabeth Hurley	707
Elly Gregoric	695
Em Støy	395
Emma Bowd	101
Emma Shields	688
Employment Hero	500
Endpoint Strategy Pty Ltd (trading as Test-Ed)	342
Eolas Medical	155
Erin McMullen	737
eSafety Commissioner	185
EY Australia	418
Felix O'Neill-Pugh	249
FinTech Australia	578

Participants	Sub no.
Fiona Wood	370
Fiorella Fabian	326
Fortinet	562
Frank Burgers	61
Free TV Australia	10, 770
Freya Davies-Ardill	669
Future Smart Strategies	117
Future State Studios	493
Gaetan Selle	201
Georgia Manwaring	745
Getty Images	262
Global Legal Entity Identifier Foundation (GLEIF)	265
Global Shield Australia	329
Good Ancestors	169
Good Things Foundation Ltd (Good Things Australia)	521
Google Australia and New Zealand	32
Governance Institute of Australia Ltd	28
Grace Chan	702
Gradient Institute	401
Great Bowery T/A MAP or B&A Reps (MAP and B&A Reps)	310, 336, 345
Greg Strangman	529
Group of 100 (G100)	1, 363
GS1 Australia	9, 415
Guardian Australia	540
Guy Cunningham	210
Hachette Australia Pty Ltd (Hachette Australia)	306
Hannah Diviney	270
Harry Dowling	248
Harry Wu	189
Hayley Boyce	243
Hazel Kinnear	303
HeapsGood Music	121
Heather Rose	446

Participants	Sub no.
Heavy Vehicle Industry Australia (HVIA)	6, 552
Henry Freeman-Dick	235
Holden Sheppard	402
Hugh McFarlane	110
Human Technology Institute (HTI)	344
HumanAbility	3, 514
IAB Australia (IAB)	601
Ian Ferrington Michaelis	472
ICON Management Pty Ltd (ICON Management)	82
IFPI	312
Image Makers Association Australia (IMAA)	385
Independent Schools Australia (ISA)	771
India Cowie-Kent	338
Indigenous Art Centre Alliance	577
Indigenous Art Code Ltd	130
Indigenous Literacy Foundation (ILF)	263
Infrastructure Victoria	290
Ingrid Purnell	144
Inkspot Bookshop	120
Institute of Professional Editors Limited (IPEd)	421
Institute of Public Accountants (IPA)	481
Insurance Council of Australia (ICA)	330
Interactive Games & Entertainment Association (IGEA)	313
International Affiliation of Writers Guilds (IAWG)	543
International Authors Forum (IAF)	267
International Centre for Missing and Exploited Children Australia (ICMEC Australia)	416
International Confederation of Societies of Authors and Composers (CISAC)	451
International Federation of Reproduction Rights Organisations (IFRRO)	378
International Organization for Standardization (ISO)	196
Internet Association of Australia Ltd (IAA)	531
IPA, ACP, BOEV, FEP, UK PA, SNEL, SBPA, STM, SNE	468
Ironbark Photography	280

Participants	Sub no.
Isadore Farnworth	653
Isha Chhabhadia	729
ITS Australia	428
Jacinta Sassine	580
Jack Gaby	228
Jackie Wong	104
Jacqueline Saskia Heeb	734
James Clark	661
James Crothers	245
James Mackay	64
James Newson	390
James Trevelyan	97
Jamie Freestone	187
Jamila Choubassi	205
Jane Bowland	88
Jane Hogan	387, 389
Jane Orme	639
Jay Bailey	391
Jaya Pimm	382
Jazz Rowe	193
Jeannie Meekins	238
Jem Splitter	655
Jesse Pascoe	640
Jessica Depiazzi	722
Jet Akkermans-Pearce	504
Joanna Stegena	216
Joe Moreau	579
John Cosstick	52
John Ferris	91
John Halsey	73
John Swinson and Trent Dalton	219
John Wiley & Sons Australia, Ltd (Wiley)	756
John Wiltshire-Butler	713
Josh Muhlback	351

Participants	Sub no.
Joshua Yuvaraj	56
Journalism Education & Research Association of Australia (JERAA)	318
Julia Pratt	663
Julie Murphy	98
Julietta Henderson	314
K Bowrey, J McKeough, K Weatherall, I Alexander, S Hook, D Simone, L Wiseman, M Handler	141
Karen Foxlee	305
Karen Ginnane	569
Karina Natt and Narelda Jacobs	252
Kate Larsen	173
Kate O'Leary	233
Kate Olsson	692
Kate Sullivan	327
Katherine Allum and Michael Burrows	332
Katherine Blackadder	615
Kelly Lewis	365
Kernl	509
Khalil Najjar	698
Kim Barden	758
Kingsley Judd	54
Konrad Biernacki	676
KPMG Australia	349
Kylie Carman-Brown	743
Lachlan Pfitzner	276
Languages and Cultures Network for Australian Universities (LCNAU)	392
Larkspur Entertainment Pty Ltd	75
Laura Cheek	668
Laura Graham	754
Laura Leighton	368
Lauren Schilling	670
Law Council of Australia	599
Leanne Wiseman	176
Lee Longmire	755

Participants	Sub no.
Lewis Coleman	664
Liam McGorry	607
Life Stories Australia (LSA)	157
Lila Swain	647
Lindsay Dullea	377
Lite n Easy	5
Loaded Brush	766
Longview Pictures Pty Ltd	380
LSEG	341
Lucas I	665
Lucie Stevens	103
Lyria Bennett Moses	526
Magabala Books Aboriginal Corporation (Magabala)	519
Maha Abed	137
Man of Many	339
Maree-Louise Evans Hill	116
Marilyn Reynolds	77
Marisa Cartland	667
Mark Jacobson	608
Master Builders Australia	34, 593
Mastercard (Australasia)	26, 775
Maurice Blackburn	24
Media, Entertainment & Arts Alliance (MEAA)	466
Medical Software Industry Association (MSIA)	487
Medical Technology Association of Australia (MTAA)	589
Medicines Australia	455
Melanie Joosten	747
Melissa Maykin	215
Mem Davis	63
Menzies Research Centre (MRC)	506
Meta	39
Michael Day (MD)	469
Michael Guihot	604

Participants	Sub no.
Michael Huang	564
Michael Noetel	171
Michael Perkins	547
Michele Lemmens	511
Michelle Prak	324
Microsoft	574
Mileva Security Labs	221
Minderoo Foundation	440
Minerals Council of Australia (MCA)	590
Monica Bowdler	289
MortarCAPS Higher Learning Data Standard Ltd (MortarCAPS)	80
Mortgage and Finance Association of Australia (MFAA)	532
Mountain District Radio Inc (3MDR)	71
Murray Bridge News (MB News)	66
MYSKILLSmanager	376
Nadine Honson	633
Natacha Murphy	651
Natalie Astwood	207
National and State Libraries Australasia Inc (NSLA)	325
National Association for the Visual Arts Ltd (NAVA)	393
National Association of Testing Authorities (NATA)	105
National Australia Bank (NAB)	581
National Electrical and Communications Association (NECA)	11
National Farmers' Federation (NFF)	585
National Growth Areas Alliance (NGAA)	553
National Tertiary Education Union (NTEU)	444
NewDirection Care	20
News Corp Australia (NCA)	475
News/Media Alliance (N/MA)	268
Nicholas Coghlan	768
Nicholas O'Dwyer	149
Nicki Black	727
Nicolas Palmer	334
Nicole Malm	192

Participants	Sub no.
Nik Samoylov	68
Nikita Vanderbyl	274
NSW Information and Privacy Commission (NSW IPC)	537
Office for the Arts, Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts (Office for the Arts)	588
Office of the Australian Information Commissioner (OAIC)	356
Office of the Information Commissioner (Qld) (OIC)	445
Office of the Victorian Information Commissioner (OVIC)	761
Oliver Burford	672
Oliver Chang	645
Olivia Jones	725
Open ID Foundation – Australian Digital Trust Community Group (OIDF ADTCG)	462
Oxford University Press (OUP)	539
Patrick Moroney	650
Patrick Stokes	160
Paul Greene	251
Paul Murray	53
Paul White	508
PauseAI Australia (PauseAI)	297
Penelope Hyde	225
Penguin Random House Australia Pty Ltd (Penguin Random House Australia)	477
Per Capita Centre of the Public Square	283
Pete Reid	457
Peter Barry	681
Peter Butler	545
Peter Garrett	122
Peter Holberton	612
Peter Horniak	439
Peter Leonard	100, 183, 411
Peter McLarty	683
Peter Sardi	403
Phillip Healey	461
Population Health Research Network (PHRN)	603
Public Skills Australia	530

Participants	Sub no.
QMusic	266
Rachel McCann	109
Rebecca Oyomopito	143
Reginald Ashman	716
Regional Australia Institute (RAI)	13, 557
RELX	226
Research Australia	525
Revealr.ai (the trading name of Wordflow Pty Ltd) (Revealr)	496
Rhiân Williams	320
Rhianna Nelson	697
Robert Broad	190
Robyn Lawley	132
Roisin O'Donovan	718
Rory Fraser-Peckham	162
Royal Australian College of General Practitioners (RACGP)	773
Russell Tassicker	48
Ryan Penning	690
Sam Chilton	209
Sam Coggins	292
Sam Mularczyk	656
Samuel Edmonds	458
Samuel L'Huillier	634
Samuel Richards	92
Sarah Armstrong	646
Sarah-Jo Lobwein	674
Scarlett Maxwell	129
Scholastic Australia Pty Ltd	323
Science & Technology Australia	559
Screen Producers Australia (SPA)	45
Screenrights	352
Seafood Consumers Association Ltd (SCA)	134
Sean Figgers	492
Seer Data & Analytics	408
Serge Thomann	239

Participants	Sub no.
Sezoo Pty Ltd (Sezoo)	406
Shaun Wilson	371
Shayne O'Neill	51
Shivaun Sutcliffe	118
Simon Kearns	65
Simon Kneebone	573
Skyscanner Limited (Skyscanner)	197
Small Press Network (SPN)	293
Sneha Joshi	701
Society of Children's Book Writers & Illustrators (SCBWI)	108
Sony Music Entertainment Australia Pty Ltd (Sony Music Australia)	429
Sophie Drodge	714
Sophie Miller	735
Sophie Sardi	208
Sovereign Australia AI Pty Ltd	125
Special Broadcasting Corporation (SBS)	448
Spinifex Press Pty Ltd (Spinifex Press)	538
SRI4GoodAI	206
Stephanie Gemmill	113
Steven Robinson	69
Stewart Webb	733
Stirling & Rose	269
Sue Bond	158
Sue Holmes	548
Sumit Chowdhury	47
Suzannah Arnot	112
Tahlee Rouillon	409
Tahlia Ludlow	240
Tahnya Donaghy	76
Talitha Fraser	150
Taylor & Francis	302

Participants	Sub no.
Tech Council of Australia (TCA)	534
Tech Femme Fusion	369
Telecommunications Industry Ombudsman (TIO)	407
Telstra	36, 586
Terri Janke and Company	436
Tessa Cole	164
Tessie Overmyer	644
The Group of Eight (Go8)	41, 499
The Independent Music Publishers International Forum (IMPF)	254
The International Confederation of Music Publishers (ICMP)	398
The Naher Agency	400
The Pharmacy Guild of Australia	29
The Smith Family	23
Therapeutic Guidelines Limited	242
Thomas Nightingale	570
Tiffany Ford-Flynn	609
Tim Davidson	86
Tim Fatchen	67
Tim Singleton Norton	135
Tim Walshaw	544
Timothy Sneddon	298
Tony Bonner	159
Trish Talob	154
UNICEF Australia	167
United Workers Union (UWU)	520
Universities Australia (UA)	510
University of Melbourne Master of Arts and Cultural Management Master of Publishing and Communications	431
University of New South Wales (UNSW)	760
UNSW AI Institute (UNSW.ai)	133
UTS Centre for Media Transition (CMT)	420
UTS Law Privacy Group	425

Participants	Sub no.
Valeriy Ogienko	81
Venture Insights Pty Ltd (Venture Insights)	178
Verity Croker	140
Warwick Holt	381
WeMoney	597
Wendy Lewis	151
Wendy Rapee	161
Wesfarmers	592
Western Australian AI Hub (WA AI Hub)	551
Westpac Group	413
William Cook	147
WiseList Pty Ltd (WiseList)	774
Woolworths Group	7, 596
Word Ninjas	497
Workday Australia (Workday)	309
Working with Women Alliance and National Aboriginal and Torres Strait Islander Women's Alliance (WWWA and NATSIWA)	186
XBRL International, Inc (XBRL International)	260
Xero	355
Zac Broeren	175
Ze Zanos	658
Zeke Coady	181
Anonymous	55
Anonymous	57
Anonymous	58
Anonymous	59
Anonymous	70
Anonymous	74
Anonymous	78
Anonymous	96
Anonymous	99
Anonymous	102
Anonymous	107
Anonymous	111

Participants	Sub no.
Anonymous	128
Anonymous	131
Anonymous	136
Anonymous	142
Anonymous	146
Anonymous	166
Anonymous	172
Anonymous	174
Anonymous	179
Anonymous	188
Anonymous	198
Anonymous	204
Anonymous	213
Anonymous	218
Anonymous	220
Anonymous	222
Anonymous	223
Anonymous	224
Anonymous	227
Anonymous	229
Anonymous	230
Anonymous	231
Anonymous	232
Anonymous	237
Anonymous	246
Anonymous	253
Anonymous	255
Anonymous	256
Anonymous	257
Anonymous	258
Anonymous	261
Anonymous	271
Anonymous	273
Anonymous	275

Participants	Sub no.
Anonymous	277
Anonymous	278
Anonymous	281
Anonymous	294
Anonymous	296
Anonymous	299
Anonymous	300
Anonymous	304
Anonymous	315
Anonymous	316
Anonymous	321
Anonymous	328
Anonymous	335
Anonymous	340, 353
Anonymous	346
Anonymous	347
Anonymous	357
Anonymous	359
Anonymous	372
Anonymous	375
Anonymous	388
Anonymous	405
Anonymous	419
Anonymous	423
Anonymous	427
Anonymous	430
Anonymous	433
Anonymous	434
Anonymous	435
Anonymous	437
Anonymous	441
Anonymous	442

Participants	Sub no.
Anonymous	450
Anonymous	452
Anonymous	453
Anonymous	454
Anonymous	456
Anonymous	459
Anonymous	460
Anonymous	467
Anonymous	470
Anonymous	471
Anonymous	474
Anonymous	476
Anonymous	480
Anonymous	483
Anonymous	486
Anonymous	491
Anonymous	503
Anonymous	507
Anonymous	527
Anonymous	550
Anonymous	606
Anonymous	610
Anonymous	617
Anonymous	619
Anonymous	620
Anonymous	621

Participants	Sub no.
Anonymous	622
Anonymous	623
Anonymous	624
Anonymous	625
Anonymous	626
Anonymous	627
Anonymous	628
Anonymous	629
Anonymous	630
Anonymous	631
Anonymous	632
Anonymous	636
Anonymous	637
Anonymous	638
Anonymous	641
Anonymous	643
Anonymous	648
Anonymous	649
Anonymous	652
Anonymous	654
Anonymous	657
Anonymous	659
Anonymous	666
Anonymous	677
Anonymous	682
Anonymous	684
Anonymous	685
Anonymous	687
Anonymous	689
Anonymous	691
Anonymous	693
Anonymous	694

Participants	Sub no.
Anonymous	696
Anonymous	699
Anonymous	700
Anonymous	703
Anonymous	705
Anonymous	706
Anonymous	712
Anonymous	715
Anonymous	719
Anonymous	720
Anonymous	723
Anonymous	724
Anonymous	726
Anonymous	728
Anonymous	730
Anonymous	732
Anonymous	736
Anonymous	738
Anonymous	739
Anonymous	744
Anonymous	746
Anonymous	748
Anonymous	750
Anonymous	751
Anonymous	752
Anonymous	753
Anonymous	763
Anonymous	764
Anonymous	765
Anonymous	772

Table A.4 – Questionnaire responses

Participants	qr no.
Aidan O'Shaughnessy	2
Atlassian Pty Ltd	50
ATN Universities	13
Australasian Performing Right Association and Australasian Mechanical Copyright Owners Society (APRA AMCOS)	58
Australian Copyright Council (ACC)	72
Australian Digital Health Agency (ADHA)	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 (APA and ASA)	39
Australian Recording Industry Association of Australia and the Phonographic Performance Company of Australia Ltd (ARIA and 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 Advisory Group – Schools (CAG Schools)	40
Copyright Advisory Group – TAFE (CAG TAFE)	41
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

Participants	qr no.
GS1 Australia	63
Heavy Vehicle Industry Australia (HVIA)	20
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
Moira Scerri	53
Montu Group Pty Ltd	35
Mortgage and 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
Screenrights	17
Social Ventures Australia (SVA)	26
Super Members Council (SMC)	37
Tax Justice Network Australia	42
The George Institute for Global Health	32
Tech Council of Australia (TCA)	69

Participants	qr no.
The University of Sydney	21
Uniting Church in Australia, Synod of Victoria and Tasmania	44
Visa	24
Workday Australia (Workday)	56
Xero	18
Anonymous	1
Anonymous	3
Anonymous	9
Anonymous	10
Anonymous	15
Anonymous	23
Anonymous	47

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.

Artificial intelligence (section B.2). 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.

Improved use of data (section B.3). Within the next decade, rightsizing the Consumer Data Right (CDR), outcomes-based privacy regulation and digital financial reporting (chapters 3 to 5) 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.4). 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.

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
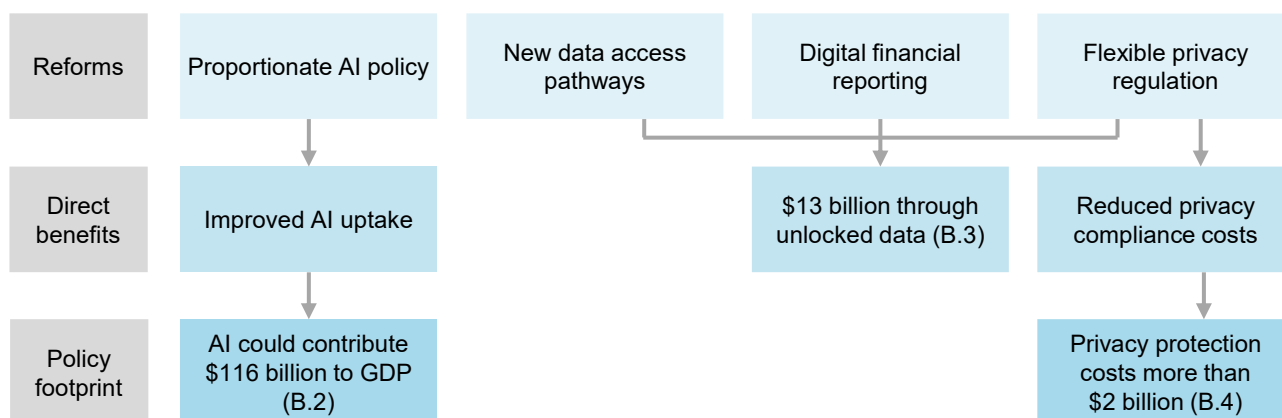
B.2   Estimating the productivity effects of AI

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. 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.1 – 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%	United States	Task-based: 4.6% of activity improved by 11.5%
Aghion and Bunel (2024)	6.8% (0.7–12.4%)	United States	Task-based: 30% of activity improved by 22.8%
Bergeaud (2024)	2.9% (1.3–4.5%)	European Union	Task-based: 17.2% of activity improved by 16.8%
Briggs and Kodnani (2023)	15% (3–30%) labour productivity	United States	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	United States	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]	European Union	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,[58] 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).

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

---

[58] 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.

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.

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

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:

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

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 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).

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

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 2025c; RBA 2025), but every 1% increase in labour productivity for the average Australian worker yields $150 a month (PC calculations based on ABS 2025f, 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%).[59] That is:

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

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 half will only reduce labour costs. Given the 53% labour share in Australia (ABS 2025e),[60] this implies 16.4% gains in multifactor productivity.

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

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.1). For example, US survey evidence suggests AI may already be offering time savings amounting to 1.4% of work hours (Bick et al. 2024).

---

[59] 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.
[60] 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.

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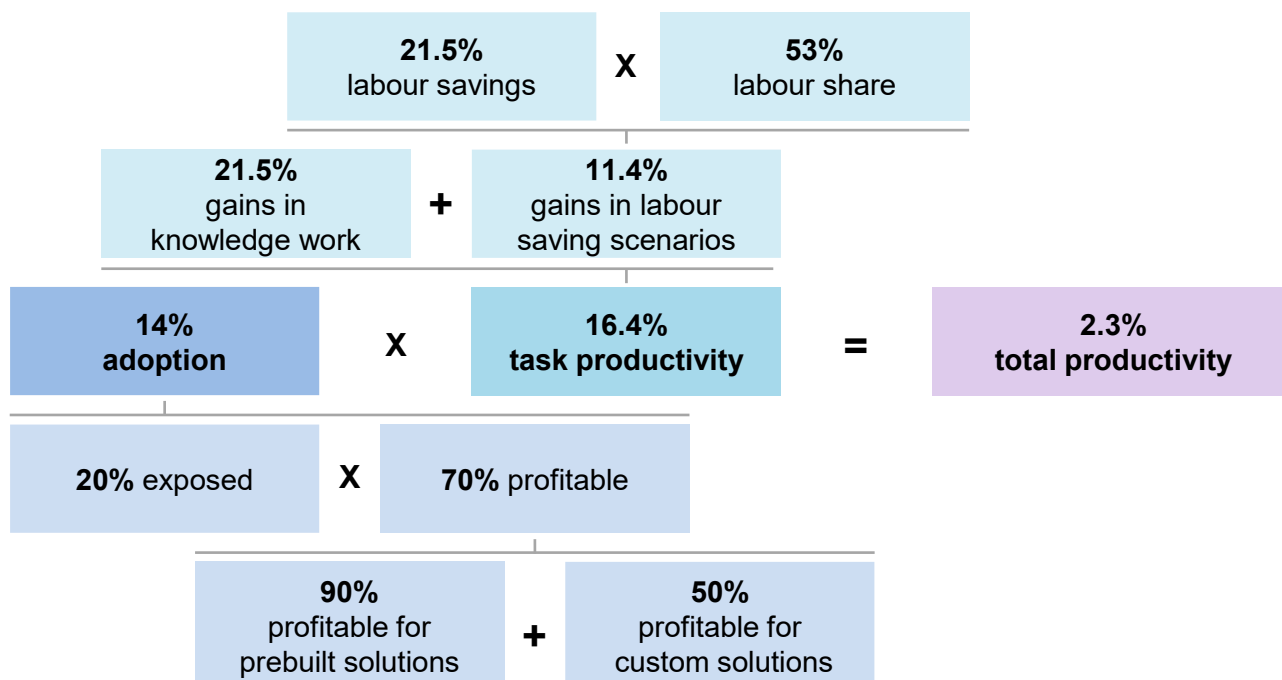
a. Numbers may not sum due to rounding. Gains in labour saving scenarios were lower than Acemoglu (2025) due to differences in the labour share.

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 2025e, table 2; equation 7). This would correspond to an additional $116 billion in GDP or $4,400 per capita (ABS 2025b, table 1). That said, there is a great deal of uncertainty.

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

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.

B.3 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.

- *Rightsizing the CDR* could 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),[61] 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.[62] However, such an approach might not account for particularly valuable uses for data.

---

[61] 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).

[62] 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 2025e, table 2) this would produce a 0.5% increase in output (% Δoutput = % Δproductivity + 0.53 $\times$ % Δlabour + 0.47 $\times$ % Δcapital and hence 0.47 $\times$ 1% = 0.47%).

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. Based on Australian data in 2024-25, this would imply a benefit worth $28 to $69 billion (ABS 2025c, tbl. 1). 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 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.[63]

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 2023a, 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 cost[64] (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.[65]

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

- *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 United States (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.

---

[63] 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.

[64] 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.

[65] For instance, if each reform contributes 10% to 75% of total benefits.

- Deloitte Access Economics (2023, p. 14) modelling suggested the benefits from the *digital financial report* data of large Australian companies[66] may add $6 billion to GDP (non-data related benefits could add an additional $1.7 billion).

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 credit[67] and increased competition (OECD 2021).

B.4 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.3). 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

---

[66] 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 2018a).

[67] 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).

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.

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 five[68] to account for the fact that the IAPP-EY sample was focused on privacy active firms.[69]

Findings

These estimates imply a cost on the order of $2 billion annually for the estimated 10,000 businesses[70] with turnover of at least $50 million who hold personal information. 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 billion[71] 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.[72]

Limited evidence is available for the costs among the estimated 267,000 businesses[73] 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.

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.

---

[68] 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.

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

[70] 6,303 + 3,108 + 679 (table B.2).

[71] 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.

[72] 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.2 implies at least $1.46 trillion, or at least 28%.

[73] 159,000 + 107,575 (table B.2).

- **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.

Table B.2 – 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, 2025d), DSIT (2024), World Bank (2025).

C. International AI regulation

The following table C.1 lists the status of regulation directly related to artificial intelligence (AI) in each of the 38 core OECD countries, as at December 2025. Population and gross domestic product (GDP) estimates are also included in the table to illustrate the size of each nation's economy.

Table C.1 – Status of AI legislation in OECD countries

Jurisdiction	AI regulation status	AI regulation details	Population (2024)	GDP (millions, current international PPP adjusted in 2024)	Name of instrument
Australia	No legislation introduced to parliament or passed	A mandatory guardrails proposal paper was released in 2024 (DISR 2024b), but a bill has not yet been tabled in parliament.	27,204,809	1,936,798	N/A
Austria	Passed and broad-based	Member of the European Union (EU), subject to the same Act as other EU countries (EU 2025).	9,178,482	657,344	EU Artificial Intelligence Act (Regulation (EU) 2024/1689)
Belgium	Passed and broad-based	Member of the European Union, subject to the same Act as other EU countries (EU 2025).	11,876,844	856,629	EU Artificial Intelligence Act (Regulation (EU) 2024/1689)
Canada	Regulation introduced to parliament (over 12 months ago) but not yet passed	An AI act was introduced June 2022, but the passage of the legislation stalled when parliament was prorogued earlier this year (Duball 2025; Fraser and Anderson Dykema 2025).	41,288,599	2,702,880	Bill C-27, Digital Charter Implementation Act, 2022 (Parliament of Canada)
Chile	Regulation introduced to parliament (over 12 months ago) but not yet passed	The Bill was introduced to parliament in May 2024 (MinCiencia nd), and has been presented to Chile's second house for debate.	19,764,771	684,595	Proyecto de Ley que regula los sistemas de Inteligencia Artificial [Bill regulating Artificial Intelligence systems] (Chile)

Jurisdiction	AI regulation status	AI regulation details	Population (2024)	GDP (millions, current international PPP adjusted in 2024)	Name of instrument
Colombia	Regulation proposed/introduced to parliament (less than 12 months ago) but not yet passed	A full AI Bill was introduced to parliament in May 2025 (MinCiencias 2025).	52,886,363	1,136,771	Proyecto de Ley Nº 422 de 2025 Senado, "Por medio de la cual se establece el marco legal para la promoción, desarrollo y uso responsable de la inteligencia artificial en Colombia" [Senate Bill No. 422 of 2025, "Establishing the legal framework for the promotion, development and responsible use of artificial intelligence in Colombia"] (Colombia)
Costa Rica	Regulation introduced to parliament (over 12 months ago) but not yet passed	There are three bills at present (Morrison Foerster nd): • Expediente 23.771: currently under review by a legislative committee (commission) (Introduced 30 May 2023) • Expediente 23.919: progressed beyond the commission to the assembly (Introduced 6 Sept 2023) • Expediente 24.484: currently under review by the commission (Introduced 6 Aug 2024)	5,129,910	154,220	• Expediente 23.771: Ley de Regulación de la Inteligencia Artificial en Costa Rica [Law Regulating Artificial Intelligence in Costa Rica] (Costa Rica) • Expediente 23.919: Ley para la Promoción Responsable de la Inteligencia Artificial en Costa Rica [Law for the Responsible Promotion of Artificial Intelligence in Costa Rica] (Costa Rica) • Expediente 24.484: Ley para la Implementación de Sistemas de Inteligencia Artificial [Law for the Implementation of Artificial Intelligence Systems] (Costa Rica)
Czechia	Passed and broad-based	Member of the European Union, subject to the same Act as other EU countries (EU 2025).	10,882,164	618,168	EU Artificial Intelligence Act (Regulation (EU) 2024/1689)
Denmark	Passed and broad-based	Member of the European Union, subject to the same Act as other EU countries (EU 2025).	5,976,992	475,256	EU Artificial Intelligence Act (Regulation (EU) 2024/1689)
Estonia	Passed and broad-based	Member of the European Union, subject to the same Act as other EU countries (EU 2025).	1,371,986	67,685	EU Artificial Intelligence Act (Regulation (EU) 2024/1689)
Finland	Passed and broad-based	Member of the European Union, subject to the same Act as other EU countries (EU 2025).	5,637,214	361,296	EU Artificial Intelligence Act (Regulation (EU) 2024/1689)
France	Passed and broad-based	Member of the European Union, subject to the same Act as other EU countries (EU 2025).	68,516,699	4,201,560	EU Artificial Intelligence Act (Regulation (EU) 2024/1689)

Jurisdiction	AI regulation status	AI regulation details	Population (2024)	GDP (millions, current international PPP adjusted in 2024)	Name of instrument
Germany	Passed and broad-based	Member of the European Union, subject to the same Act as other EU countries (EU 2025).	83,510,950	6,037,852	EU Artificial Intelligence Act (Regulation (EU) 2024/1689)
Greece	Passed and broad-based	Member of the European Union, subject to the same Act as other EU countries (EU 2025).	10,388,805	457,879	EU Artificial Intelligence Act (Regulation (EU) 2024/1689)
Hungary	Passed and broad-based	Member of the European Union, subject to the same Act as other EU countries (EU 2025).	9,562,314	455,509	EU Artificial Intelligence Act (Regulation (EU) 2024/1689)
Iceland	No legislation introduced to parliament or passed	Has signed the Council of Europe Framework Convention on AI (Council of Europe nd). As of December 2025, the convention has not been ratified through Iceland's own parliament.	404,610	31,664	Council of Europe Framework on Artificial Intelligence and Human Rights, Democracy and the Rule of Law
Ireland	Passed and broad-based	Member of the European Union, subject to the same Act as other EU countries (EU 2025).	5,380,257	705,756	EU Artificial Intelligence Act (Regulation (EU) 2024/1689)
Israel	No legislation introduced to parliament or passed	Only measures to incentivise AI development have been introduced, and no Bill has been introduced to regulate AI's use or development (Or-Hof 2024).	9,974,400	555,482	N/A
Italy	Passed and broad-based	Member of the European Union, subject to the same Act as other EU countries (EU 2025).	58,986,023	3,589,122	EU Artificial Intelligence Act (Regulation (EU) 2024/1689)
Japan	Passed and narrow	On 28 May 2025, the Bill was approved by Japan's Parliament. The Act has been described as 'broad' and 'high-level', and does not impose specific penalties for non-compliance (Clifford Chance 2025).	123,975,371	6,407,672	Act on the Promotion of Research and Development, and Utilization of AI-related Technology, Act No. 53 of 2025 (Japan)
Latvia	Passed and broad-based	Member of the European Union, subject to the same Act as other EU countries (EU 2025).	1,862,441	81,700	EU Artificial Intelligence Act (Regulation (EU) 2024/1689)
Lithuania	Passed and broad-based	Member of the European Union, subject to the same Act as other EU countries (EU 2025).	2,888,055	157,151	EU Artificial Intelligence Act (Regulation (EU) 2024/1689)

Jurisdiction	AI regulation status	AI regulation details	Population (2024)	GDP (millions, current international PPP adjusted in 2024)	Name of instrument
Luxembourg	Passed and broad-based	Member of the European Union, subject to the same Act as other EU countries (EU 2025).	677,717	102,181	EU Artificial Intelligence Act (Regulation (EU) 2024/1689)
Mexico	Regulation introduced to parliament (over 12 months ago) but not yet passed	An AI Bill was introduced in April 2025, and is currently under deliberation in the Senate (Goodrich 2025).	130,861,007	3,361,570	Ley Federal para el Desarrollo Ético, Soberano e Inclusivo de la Inteligencia Artificial [Federal Law for the Ethical, Sovereign and Inclusive Development of Artificial Intelligence] (Mexico)
Netherlands	Passed and broad-based	Member of the European Union, subject to the same Act as other EU countries (EU 2025).	17,994,237	1,515,447	EU Artificial Intelligence Act (Regulation (EU) 2024/1689)
New Zealand	No legislation introduced to parliament or passed	'New Zealand is taking a light-touch and principles-based approach to AI policy. New Zealand has existing regulatory frameworks' (Ministry of Business, Innovation and Employment (NZ) 2025, p. 10).	5,338,500	294,117	N/A
Norway	Regulation proposed/introduced to parliament (less than 12 months ago) but not yet passed	Norway announced steps to align with the EU AI Act in March 2025 (Ministry of Digitalisation and Public Governance (Norway) 2025). As at December 2025, legislation has not yet been introduced into parliament, but a draft AI Act has been released for consultation (DFD 2025).	5,572,272	562,975	N/A
Poland	Passed and broad-based	Member of the European Union, subject to the same Act as other EU countries (EU 2025).	36,554,707	1,841,555	EU Artificial Intelligence Act (Regulation (EU) 2024/1689)
Portugal	Passed and broad-based	Member of the European Union, subject to the same Act as other EU countries (EU 2025).	10,701,636	541,680	EU Artificial Intelligence Act (Regulation (EU) 2024/1689)
Slovak Republic	Passed and broad-based	Member of the European Union, subject to the same Act as other EU countries (EU 2025).	5,422,069	255,818	EU Artificial Intelligence Act (Regulation (EU) 2024/1689)
Slovenia	Passed and broad-based	Member of the European Union, subject to the same Act as other EU countries (EU 2025).	2,126,324	120,202	EU Artificial Intelligence Act (Regulation (EU) 2024/1689)

Jurisdiction	AI regulation status	AI regulation details	Population (2024)	GDP (millions, current international PPP adjusted in 2024)	Name of instrument
South Korea	Passed and broad-based	The AI Basic Act was passed on December 26, 2024. Legislation was first tabled in the National Assembly in July 2020, and the law will take effect in January 2026 (Ministry of Science and ICT (South Korea) 2024).	51,751,065	2,699,604	Act on the Development of Artificial Intelligence and Establishment of Trust [Artificial Intelligence Basic Act] (Republic of Korea)
Spain	Passed and broad-based	Member of the European Union, subject to the same Act as other EU countries (EU 2025).	48,807,137	2,778,407	EU Artificial Intelligence Act (Regulation (EU) 2024/1689)
Sweden	Passed and broad-based	Member of the European Union, subject to the same Act as other EU countries (EU 2025).	10,569,709	750,771	EU Artificial Intelligence Act (Regulation (EU) 2024/1689)
Switzerland	Regulation proposed/introduced to parliament (less than 12 months ago) but not yet passed	Switzerland have stated that they will ratify the council of Europe convention on AI (News Service Bund 2025b, 2025a), but intend to make 'limited sector-specific adjustments to existing laws and limiting general, cross-sector regulation to key areas relevant to fundamental rights, such as data protection' (Dal Molin et al. 2025).	9,034,102	847,568	N/A
Turkiye	Regulation introduced to parliament (over 12 months ago) but not yet passed	Draft proposal has been submitted to the Turkish grand national assembly in June 2024 (Kosterit 2025).	85,518,661	3,757,013	Yapay Zekâ Kanun Teklifi [Artificial Intelligence Bill] (Turkiye)
United Kingdom	Regulation proposed/introduced to parliament (less than 12 months ago) but not yet passed	Draft legislation introduced in the House of Lords in March 2025. There has been limited progress since (Courea and Stacey 2025).	69,226,000	4,196,506	Artificial Intelligence (Regulation), Bill [HL] 30 (United Kingdom)
United States - California[a]	Passed and narrow	California introduced an AI Act in September 2025. The Act is privacy and transparency focused, and does not legislate broadly to manage risk levels or save for those classed catastrophic (Singer and Phillips-Robins 2025).	39,431,263	4,032,478[b]	Senate Bill 53 (Cal.), Chapter 138, Transparency in Frontier Artificial Intelligence Act (State of California)
United States - Colorado[a]	Passed and broad-based	Colorado passed AI legislation in May 2024. The Act could be considered broad, as it legislates using risk levels. Implementation of the Act has been	5,957,493	555,480[b]	Colorado Revised Statutes Annotated, Title 6, Article 1, Part 17, Colorado Artificial Intelligence Act (State of Colorado)

Jurisdiction	AI regulation status	AI regulation details	Population (2024)	GDP (millions, current international PPP adjusted in 2024)	Name of instrument
		delayed to June 2026 (Langehennig 2025).			
United States - Texas[a]	Passed and narrow	Legislation was introduced in Texas in June 2025 and comes into force on January 1, 2026. Like California and Utah, the legislation is disclosure focused but prohibits some high-risk uses (such as social scoring and intentional discrimination) (Martinez 2025).	31,290,831	2,759,072[b]	House Bill 149, Texas Responsible Artificial Intelligence Governance Act (State of Texas)
United States - Utah[a]	Passed and narrow	Utah passed legislation that took effect in May 2024 (Levi et al. 2024). The legislation is similar to California in that it is disclosure focused.	3,503,613	298,315[b]	Senate Bill 149, Artificial Intelligence Policy Act. (State of Utah)
United States - Other 46 States	No legislation introduced to parliament or passed	Some states have regulations relevant to AI in specific domains, but do not directly regulate the technology itself (Dawson et al. 2025). There is no federal level legislation to regulate the use or development of AI (Library of Congress 2025).	259,927,788	21,539,545	N/A

a. Given the large populations and GDP of some US states and their separate approaches to AI legislation, they have been included at the bottom of the table. **b.** US state GDP figures are calculated as a share of the World Bank's estimates of national GDP (2024a). However, the share that each state makes up here is calculated according to the state's share of national GDP as estimated by the U.S Bureau of Economic Analysis in 2024. These shares are then multiplied by the World Bank's 2024 national GDP figure for the final estimate of state GDP, in order to maintain consistency.

Sources: United States Census Bureau (2024), U.S. Bureau of Economic Analysis (2025), World Bank (2024b, 2024a).

D. Effect of AI on creators' incentives to produce content

Artificial intelligence (AI) could affect the incomes of content creators in several ways – some positive and some negative.

On the positive side, AI is expected to boost overall productivity which could lift average incomes and increase demand for creative content, whether made by people or by AI. AI can also help creators work more efficiently by supporting or automating parts of the creative process (augmentation), which may raise their incomes. Furthermore, some AI companies are now paying for access to human-created content to train their models (chapter 2). These agreements could raise demand for such content and offer creators an extra source of income.

On the other hand, AI-generated content can also compete with human-made work (automation), potentially lowering demand for some types of human-created content and reducing creator incomes.

Overall, it is still uncertain whether AI will increase or reduce creator incomes.

If the income creators receive from producing new content falls, their economic incentive to create that work will fall too. This could have a negative effect on productivity. AI models require new, human-made content to train on – if less new human-made content is produced, the speed at which AI models improve could slow (Getty Images, sub. 262, p. 3; Sony Music Australia, sub. 429, p. 5), decreasing the productivity growth from AI's adoption and use.

Many participants in this inquiry emphasised the capacity of AI to compete with content creators, rather than augment them (DPA, sub. 384, p. 6; IPEd, sub. 421, p. 2; John Swinson and Trent Dalton, sub. 219, p. 2). But there is evidence of the potential for augmentation. For example, Jobs and Skills Australia (JSA) estimated exposures to automation and augmentation for each of the 996 Australia and New Zealand Standard Classification of Occupations three-digit occupations (such as music professionals and photographers). Overall, only 4% of occupations have a high potential for automation while nearly 31% have a high potential for augmentation (JSA 2025b, pp. 17–19).

For creative occupations specifically, the JSA results were similar (table D.1). The average augmentation scores for most creative occupations were generally higher than their automation score. And while some creative occupations were in the upper percentiles of automation exposure, they were also in the upper percentiles of augmentation exposure. For example, while 'journalists and other writers' have one of the highest automation exposures of all the three-digit occupations (92nd percentile), it also had one of the highest augmentation exposures (75th percentile).[74]

---

[74] The JSA estimates of exposure do not necessarily forecast net outcomes for any occupation. JSA did commission computable general equilibrium modelling that would be able to make such forecasts but did not release granular results at an occupation level as was done for the exposure scores.

Table D.1 – JSA noted the potential for augmentation, not just automation, in many creative industries

Selection of occupations and their associated automation and augmentation scores

Occupation	Augmentation score (percentile)	Automation score (percentile)
Actors, dancers and other entertainers	0.58 (31st)	0.24 (28th)
Artistic directors, media producers and presenters	0.68 (62nd)	0.41 (69th)
Authors, and book and script editors	0.69 (67th)	0.54 (89th)
Film, television, radio and stage directors	0.69 (67th)	0.36 (60th)
Journalists and other writers	0.70 (75th)	0.61 (92nd)
Music professionals	0.62 (43rd)	0.23 (25th)
Photographers	0.61 (41st)	0.24 (28th)
Visual arts and crafts professionals	0.57 (29th)	0.16 (9th)

Source: JSA (2025a), percentiles calculated by the PC.

Some peak creative sector bodies have commissioned modelling that projects changes to content creators' future income due to AI. These projections generally forecast lower revenue. For example, modelling commissioned by the International Confederation of Societies of Authors and Composers predicted that creators' revenues in the music and audiovisual industries will fall by 24% and 21%, respectively, by 2028 (compared to a counterfactual with no AI) (2024, pp. 67, 83). Likewise, the Australasian Performing Right Association and Australasian Mechanical Copyright Owners Society (APRA AMCOS) commissioned modelling which forecasted that Australian and New Zealand musicians will see their revenue fall by 23% by 2028 (compared to a counterfactual of no AI) (2024, p. 10). As with any projection of the future, there is a high degree of uncertainty surrounding these figures. Ultimately, AI will cause income losses for some content creators but may raise incomes for others. Precisely who suffers the losses, how many are affected, and how large the losses turn out to be is uncertain.

D.1 It is too early to know how extensive this issue is

There is some evidence of losses to content creators

As with projections of future impacts, evidence of *current* income losses among content creators comes mainly from opt-in surveys conducted by peak bodies and collecting societies.[75] Some of these surveys indicate that losses are already occurring – one found that just over 40% of translators and just under 40% of illustrators have reported reduced income due to competition from AI (SoA 2024). The US-based National Voice Over Association's survey found that 14% of voice-over actors had lost a job to a synthetic voice in the 12 months leading up to February 2025 (2025). And the Australian Association of Voice Actors (sub. 264, p, 6) argued 'it cannot be ignored that voice actors have been seeing a downturn in income for the last 12 months'.

---

[75] Because participation in these surveys is voluntary, the results may not fully reflect the broader population. They also rely on respondents' self-assessment of reasons for income changes, which may not always be accurate.

That said, the same surveys also show that AI is being used by content creators to improve productivity. APRA AMCOS estimated that about 38% of surveyed musicians used AI in their work in 2024, and that another 13% would consider using it (2024, p. 9). The same survey found that nearly half of musicians said AI could enhance their creativity. To the extent that AI does enable creators in various industries to produce content more easily, this would be expected to have a positive effect on their overall earnings, potentially offsetting some of the risks from competition.

Webpage funding models appear to have been upended by AI

AI uptake has reduced the amount of human traffic many websites receive while increasing crawler traffic by a greater amount. This is likely reducing website owners' revenues and increasing their server costs (which tend to increase roughly in proportion to website traffic), providing tangible evidence of current losses for content creators.

Websites traditionally allow automated 'crawlers' to extract key information so that their pages appear in search engine results, providing them with visibility and traffic (Pineda 2025). This is mostly a mutually beneficial arrangement. The search engines gain useful information to optimise their search results while the websites benefit from appearing in search results, which funnel viewers to their website. With more people accessing their page, a website is able to generate more revenue through advertising, subscriptions and direct sales. A decade ago, a search engine such as Google would typically crawl a website twice for every click through (table D.2).

However, the rise of AI tools, such as chatbots that summarise online content, has disrupted this model. Human visits have fallen, likely reducing the income generated by websites. Since Google launched AI Overviews in May 2024, the share of zero-click news searches (the percent of searches resulting in no clicks from the search engine results page to other websites) steadily increased from 56% to 69% by May 2025 and organic traffic to news publishers declined (Similarweb 2025, p. 3).

At the same time, automated crawler traffic has surged as these systems scrape websites for AI training, inference or search. Cloudflare found that AI and search crawler traffic on its customers' websites was 18% higher in May 2025, compared to May 2024 (Cloudflare 2025c), and that 80% of crawling was for training AI models as of August 2025 (Cloudflare 2025b). For Google bots, the ratio of crawls to referred traffic has shifted from 2:1 to 5:1 over the past decade (table D.2).

Not only does this decline in user traffic reduce advertising and subscription revenue, the increased crawling also raises server costs, imposing new burdens on content creators without delivering the benefits that come from genuine human visitors.

Table D.2 – Google and AI chatbot crawlers have a decreased ratio of crawls

Ratio of crawls to referred visitors

Search engine/AI firm	10 years ago	1 year ago	Present
Google	2:1	6:1	5:1
OpenAI	NA	250:1	820:1
Anthropic	NA	6,000:1	32,000:1

Source: Cloudflare, personal communication, 24 October 2025.

Some web content creators are attempting to reduce the traffic from crawlers and prevent AI chatbots using the information on their pages without permission. One mechanism is through the Robots Exclusion Protocol (also called robots.txt) which allows webpages to opt out of all crawlers, including those from AI companies (Cloudflare 2025a). However, participants in this inquiry noted that compliance with robots.txt is voluntary

and it can be ignored by crawlers (Guardian Australia, sub. 540, p. 2; NCA, sub. 475, p. 7). That said, many of the largest AI developers – who also account for most of the crawler traffic – claim to respect these voluntary standards (Claude 2025; Google 2025; OpenAI 2025d).

Some solutions have recently been introduced that allow the webhost to choose which AI developers they allow to crawl their website and to block others (rather than relying on compliance with voluntary robots.txt protocols) (Allen and Newton 2025). This could form the basis for payment for access to content for crawlers. However, it may also trigger a 'war of attrition', where AI developers and those developing blocking solutions spend ever increasing amounts of resources to find sophisticated ways to overcome each other's technologies. This could result in high levels of wasteful expenditure that produce minimal societal benefit.

D.2   Indigenous Cultural and Intellectual Property

Indigenous Cultural and Intellectual Property (ICIP) refers to the 'rights Aboriginal and Torres Strait Islander people have to their heritage and culture' which may exist in relation to 'knowledge, songlines, language, dance, symbols and art as well as medicines, language, bush foods, sacred sites and ecological knowledge' (Office for the Arts 2025). ICIP differs from copyright in several key respects: it is considered to belong to communities rather than individuals and, at least in some cases, it encompasses underlying ideas rather than just the expression of those ideas (as is the case for copyright law) (PC 2022, p. 362; Terri Janke and Company 2025, p. 13). ICIP also encompasses unrecorded cultural products and ideas and is not thought to be time limited like copyright.

Currently, no Australian legislation specifically recognises or protects ICIP. Intellectual property laws can provide partial protections for some forms of ICIP (for example, copyright may subsist in an artwork or a literary work that contains a traditional motif or story), but not all ICIP (for example, copyright does not protect content 70 years after its author's death, oral stories and songs, and traditional ideas and facts) (Reconciliation Australia and Terri Janke and Company 2025, p. 2).

Several participants in this inquiry raised concerns about the risks that AI may pose to the integrity of ICIP. Some said that AI developers may use ICIP to train AI models without first obtaining free, prior and informed consent from Aboriginal and Torres Strait Islander communities, while others said that AI models may create 'fake' expressions of culture or knowledge.[76] This could erode economic opportunities for Aboriginal and Torres Strait Islander people and cause cultural harm by providing 'false or misleading information about knowledge, language and culture' and 'sharing ICIP without the relevant cultural authority to do so' (Terri Janke and Company, sub. 436, p. 4). For example, an AI model could generate artwork that may superficially appear to be of Aboriginal or Torres Strait Islander origin but is a meaningless or offensive combination of traditional motifs presented outside their relevant contexts and may compete with artwork produced by Aboriginal and Torres Strait Islander artists.

In the inquiry on *Aboriginal and Torres Strait Islander visual arts and crafts*, the Productivity Commission recommended that new legislation be introduced to formally recognise the interests of Aboriginal and Torres Strait Islander communities in their traditional cultural assets and provide legal avenues for traditional owners to enforce those interests (PC 2022, p. 35). The Australian Government has committed to doing so and the Office for the Arts is in the process of developing the legislation (Office for the Arts 2025). Given that this process is ongoing and beyond the length of this inquiry, the PC has ruled it out of scope. But we acknowledge the potential for AI to affect Aboriginal and Torres Strait Islander people over and above the effects it has on other creatives.

---

[76] ABC, sub. 350, p. 14; Indigenous Art Code, sub. 130, p. 4; Magabala, sub. 519; Terri Janke and Company, sub. 436, p. 3.

E. Data access case studies

In the *Harnessing Data and Digital Technology* interim report, the Productivity Commission sought feedback on the Australian Government establishing lower cost and flexible regulatory pathways (PC 2025c, p. 47). The outcome in mind was improving the ability of individuals or businesses to access data about them to facilitate the creation of more personalised and effective products and services.

To further consider the feasibility and potential applications of additional regulatory data access pathways we undertook two case studies looking at the existing data access environment in the digital retail and loyalty rewards sector, and the agricultural sector. The case studies summarise how these data markets operate in practice and seek to identify any data access gaps that make it difficult to put data to productive uses. The case studies are illustrative and are not intended to offer an exhaustive account of all data practices or developments within these sectors.

We relied on desktop review and stakeholder engagement, including two roundtables, questionnaire responses and submissions.
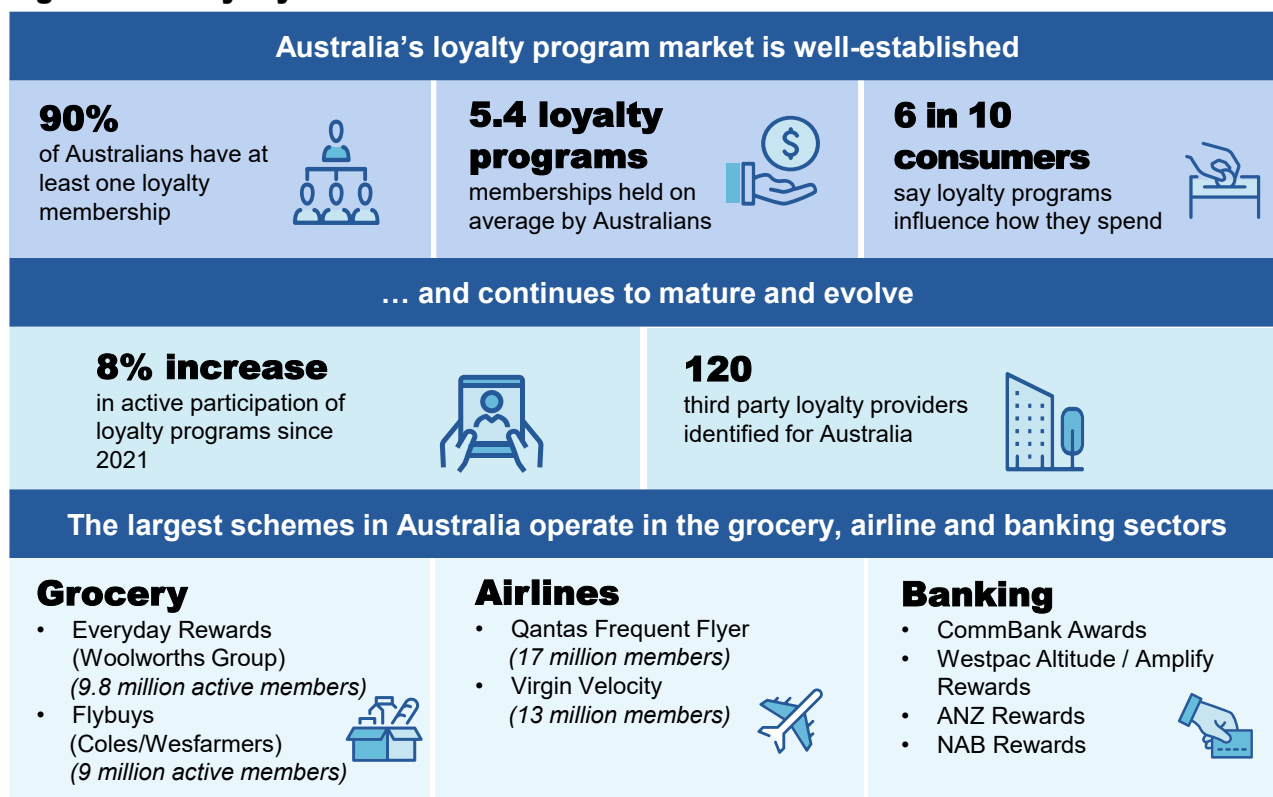
E.1 Digital retail and loyalty rewards data

Every day, Australian consumers at the supermarket, when applying for a credit card, or booking a flight are asked to create an online account or join a brand 'loyalty program'. Typically, members of loyalty programs can earn points from their online or in-store purchases at participating businesses, that can be accumulated and ultimately redeemed for a variety of rewards including products, cashback, or discounts on future purchases (ACCC 2019, pp. 1, 6).

Australia's loyalty program market is well-established (figure E.1). Recent estimates suggest that 90% of Australian consumers – 19.3 million people – are members of at least one loyalty program, with the average Australian being a member of 5.4 loyalty programs (ALA 2024). While the average number of memberships has remained stable over the past decade, active engagement has risen in recent years: since 2021 'members presenting their card at purchase' has increased by 8% (The Point of Loyalty 2025, p. 13).

Some businesses – such as Qantas Frequent Flyer and Flybuys (owned jointly by Coles Group and Wesfarmers) – own and operate their loyalty programs primarily through dedicated subsidiaries, while others engage third-party providers to outsource capability for some, or all aspects of the service offering (Ellipsis 2024; Loyalty & Reward Co 2019, p. 26; Qantas 2024, p. 27; Wesfarmers 2025). There are 120 third-party loyalty options available to Australian companies (Ellipsis 2024). Woolworths, Bakers Delight, Freedom and Kathmandu are examples of retailers that use a third-party platform to operate aspects of their loyalty program (Ellipsis 2024).

Figure E.1 – Loyalty schemes in Australia

Australia's loyalty program market is well-established

90%
of Australians have at least one loyalty membership

5.4 loyalty programs
memberships held on average by Australians

6 in 10 consumers
say loyalty programs influence how they spend

… and continues to mature and evolve

8% increase
in active participation of loyalty programs since 2021

120
third party loyalty providers identified for Australia

The largest schemes in Australia operate in the grocery, airline and banking sectors

Grocery
- Everyday Rewards (Woolworths Group) *(9.8 million active members)*
- Flybuys (Coles/Wesfarmers) *(9 million active members)*

Airlines
- Qantas Frequent Flyer *(17 million members)*
- Virgin Velocity *(13 million members)*

Banking
- CommBank Awards
- Westpac Altitude / Amplify Rewards
- ANZ Rewards
- NAB Rewards

Sources: ACCC (2019, p. 9); ALA (2024, p. 17); Bradney-George (2024); CK (2025); Ellipsis (2024); Loyalty Pty Ltd (2024); The Point of Loyalty (2025, p. 13); Virgin Australia (2025); White Label Loyalty (2024).

Loyalty programs capture extensive and detailed data about consumers

Setting up a loyalty account typically involves providing basic information about who you are (for example, name and date of birth), your contact details (for example, email, phone and address) and demographic details (for example, gender) (Loyalty & Reward Co 2019, p. 40). Loyalty programs are often linked or integrated into a retailer's e-commerce platform (for example, an online shopping app).

While digital customer accounts collect data necessary to deliver core services – such as billing information to process an online order – loyalty programs are typically designed to collect additional data that can be used to produce insights about customer behaviour (ACCC 2019, p. 45; Loyalty & Reward Co 2019, p. 3).

And indeed data collected by loyalty programs can facilitate the creation of very rich information datasets about consumers (table E.1), including purchase information drawn from linked online shopping accounts (ACCC 2019, p. 40). These datasets can offer insights into a customer's shopping patterns and preferences (for example, what they buy and when) but also about their broader behaviours and interests (ACCC 2019).

Table E.1 – Examples of information collected/ used by Flybuys and Everyday Rewards

	Flybuys	Everyday Rewards
Account details	• Name, contact information (such as email, mobile number, address, date of birth, gender).	• Name, email, mobile, residential/delivery address, date of birth, Everyday Rewards Card number.
Membership / linked accounts and partners	• Added members, connection between memberships, communications records, survey or competition responses. • Data from service providers (for example, Coles and Wesfarmers group companies) who administer Coles branded products and services (for example, payment cards and insurance) and other third parties who help to run the Flybuys program (for example, technology, media and advertising services).	• Payment card and family members linked to Everyday Rewards transactions, online services and other linked offerings (for example, mobile or insurance). • Data from Everyday Rewards Partners, other service providers (for example, Australia Post) and other parties (for example, Endeaver Group). • Data from validation services (for example, financial services and telecommunications organisations) for fraud and scam prevention.
Transactions and purchases	• Payment/transaction history (for example, what, when, where, quantity and offers activated) including in-store purchases. • Payment method and card used. • Points accrual/redemption and reward details (for example, any offers you activate and qualify for in that transaction and details of any rewards you redeemed points for in that transaction).	• Orders/purchases (for example, what, how, when), including in-store purchases. • Point accrual, use and reward details. • Payment data. • Identification (for example, driver's license, if provided).
Browsing data	• Website/app interactions and information collected by cookies, pixels and other technologies (for example, IP address, device/browser info; online behaviour).	• Browsing behaviour on Woolworths/Everyday sites/apps; promotions activated, items added to cart, device ID, browser type and version, location data.
Generated / inferred	• Information about customer preferences/interests for analytics, segmentation, research purposes, modelling and targeted advertising. • Analytics/ insights may be shared with Flybuys partners (for example, Coles), suppliers (for example, Google, Adobe, LiveRamp, Pinterest, TikTok, and Meta) and other third parties (for example, analytics service providers, media, technology and advertising companies).	• Information about customer preferences/interests. • Analytics/insights and other information may be shared to Woolworths Group (for example, Everyday Insurance), Everyday Rewards Partners (for example, Qantas, Ampol and BWS), suppliers and other parties (for example, Google, Meta).

Sources: ACCC (2025b); Everyday Rewards (2024); Flybuys (2025b); Page (2021); Woolworths Group (2025c)

How do loyalty programs use their data holdings?

Loyalty programs are used by retailers to drive repeat customers (ACCC 2019, pp. 90–91). And they appear to work. Just being a member of a loyalty program appears to significantly change behaviour. An Australian survey found that 60% of respondents changed their shopping behaviour – for example, they increased their purchasing frequency – simply by being a member of an organisation's loyalty program (McKinsey & Company 2023).

Loyalty firms use their data holdings to effectively target their marketing, including via individually tailored customer experiences, targeted advertisements and specific product recommendations (ACCC 2019, pp. 90–91).

Loyalty providers are increasingly adopting more sophisticated technology and investing in partnerships and app-based engagement features (ALA 2025). For example, the prevalence of coalition loyalty programs – where multiple brands collaborate to offer shared benefits – is increasing in Australia. Under these arrangements, affiliated retailers, service providers, and other companies partner with other brands to issue loyalty points to their customers in exchange for financial compensation or other mutually beneficial arrangements (ACCC 2019, p. 45; ALA 2025; CHOICE 2021). Collaborating parties often benefit from shared consumer data and expanded customer reach without the cost of developing standalone programs. In Australia, Flybuys has partnerships spanning Coles, Kmart, Target, and Liquorland (ALA 2025).

How can consumers use loyalty program data?

In addition to rewards, individuals can benefit from use of data by loyalty programs when it leads to, for example, better-targeted advertisements and expanded product offerings made available via data sharing agreements and partnerships with other businesses (ACCC 2019, p. 22; Fiorendino 2024).

There are also a variety of ways in which individuals can actively access, and subsequently on-share, data about them held by loyalty programs.

Digital receipts provide basic access

Table E.2 provides examples of accessible data for consumers for the popular Flybuys and Everyday Rewards programs.

Many loyalty providers now allow consumers to download data about their purchases through their online digital portals and account dashboards, typically in the form of a digital receipt in Portable Document Format (PDF) form. For example, Everyday Rewards members can access and download digital receipts for in-store purchases at Woolworths, BIG W and BWS up to 14 months after the transaction (Everyday Rewards 2025b). Similarly, Flybuys members can link their account with Flybuys partners, such as Coles, to access and download digital receipts (Coles 2025).

While digital receipts for individual purchases can be useful - for example, for checking transaction details, record keeping or managing returns they are not intended to enable consumers to readily compile, share or reuse the data for other purposes. Stitching together a time series of purchase history requires downloading multiple PDF receipts and manually extracting and formatting the relevant data (for example, by manually inputting it into a digital spreadsheet).

Third-party tools cater to more savvy users

Consumers can turn to a variety of unofficial third-party tools that can allow them to extract or regenerate the data held in their digital accounts. Those who are relatively tech savvy can use screen scraping to enable bulk data capture. For example, bespoke tools such as WooliesR can convert digital receipts into machine-readable formats (like JavaScript Object Notation files) (ekutilov 2025).

Those with less technological ability can use apps like WiseList – an Australian supermarket comparison app – which enables consumers to take photos of receipts and scan barcodes to facilitate price comparison and meal planning (WiseList 2025a, 2025c, 2025b). Many similar health management, meal planning and budgeting apps rely on consumers uploading their receipts or keying in the items they have purchased (Crunchr 2024; Dext 2025; MYOB 2025; ReceiptJar 2025; Xero 2024).

Table E.2 – Access to consumer data collected by Flybuys and Everyday Rewards

	Flybuys	**Everyday Rewards**
Account details	• Access/ edit personal information (including communication and email sharing preferences) via Account Details.	• Access/ edit their personal information via account settings for each Woolworths Group brand or program.
Membership / linked accounts and partners	• View and manage linked accounts (for example, Coles online, OnePass and Velocity Frequent Flyer). • User dashboards may not provide a full list of every third party who has received your de-identified personal data. • View linked accounts and additional cardholders.	• View Woolworths Group service linkages (for example, Everyday Extra subscription) and registered Everyday Rewards cards. • Close account through the program's website, app or by contacting customer support. • Customers can request access to personal information held about them by Woolworths Group. • Customers can view a list of categories of third parties their data has been shared with via the Woolworths Group Privacy Policy and Collection Notice, but not all specific entities are disclosed.
Transactions and purchases	• While transaction data is not made automatically available for download, consumers can link their respective accounts for Flybuys partners (for example, Coles and Bunnings) in the Flybuys app to get digital receipts. For example, consumers that link their Coles account and scan their 'Coles Barcode' will have access to a digital receipt for 14 months after the shop. This will include details such as purchases, total savings, PDF tax invoice, Flybuys points collected, Liquor voucher collectables and credits (like, Master Chef cookware or Curtis Stone BBQ credits). • View a summary of points earned/redeemed.	• View and download digital receipts in PDF form individually for in-store purchases at Woolworths, BIG W and BWS within 14 months of purchase. This will include details such as store location, item name, quantity, price, discounts, payment method, showing points activity and qualifying purchases and total spend. • View a summary of points earned/redeemed.
Browsing data	• Do not have access to all device- or browsing-metadata (for example, logs of browser type or internet protocol address history) through the consumer dashboard.	• Do not have access to all device- or browsing-metadata (for example, logs of browser type or IP history) through the consumer dashboard.

Source: Bunnings (2025); Coles (2025); Everyday Rewards (2024, 2025d, 2025c, 2025b, 2025a); Flybuys (2025d, 2025e, 2025a, 2025c); Woolworths Group (2025a, 2025b); Kyriakopoulos (2023) and Commission analysis.

These unofficial tools are useful, but they are unaffiliated with the original data holder and are not always perfectly reliable. Uploading individual receipts and manually entering in missing or additional data can be slow, cumbersome and potentially error prone. And solutions that rely on web scraping can break when retailers update or change their websites. WiseList highlighted these issues in their submission.

> While WiseList currently provides a vital price comparison service to Australians, our ability to do so relies on compiling publicly available, but unstructured, digital information. This indirect method is a fragile and inefficient workaround for the lack of official data access. It is vulnerable to constant website changes and struggles to capture the full picture of complex, store-specific promotions. (WiseList, sub. 774, p. 1)

Artificial intelligence (AI) is entering the field …

The development of AI has the potential to make it easier for consumers to bring together data held in various digital accounts, without it needing to be in a standardised form. To cope with a lack of standardised data fields and naming conventions between retailers, such as for product names, price comparison tools such as Grocerize – an Australian tech company – is leveraging AI-matching tools to facilitate price comparisons between major grocers (Grocerize 2025c, 2025a). Once consumers have decided what they want to buy, an add-on extension pushes these items into their online Coles or Woolworths shopping cart (Grocerize 2025b, personal communications, 4 December 2025; Riddle 2024).

Overseas, some retailers allow consumers to connect accounts to generative AI tools. For example, Walmart – a US retailer - has partnered with OpenAI to enable shopping through ChatGPT (Walmart 2025). This capability has been extended to online merchants Shopify and Etsy (OpenAI 2025b). Product information from multiple retailers - such as prices, availability, specifications, and reviews - is integrated into the ChatGPT interface, while consumer data, including expressed preferences and past interactions, informs personalised recommendations across different retail platforms.

There are innovative solutions that have emerged which enable consumers to regenerate data more seamlessly. Some smart appliances, such as refrigerators, now feature Wi-Fi connectivity and integration with smart home ecosystems. Certain models use internal cameras and AI-driven image recognition to automatically identify ingredients, supporting functions such as recipe suggestions customised to purchased items stored in the fridge (Samsung 2024).

… and screen scraping with low-risk data opens up further possibilities

There are emerging data access solutions that rely on screen scraping to retrieve information from user accounts or online portals. In the United States, tools such as Storelink enable developers to integrate account-linking flows into their apps so that users can log in to their retail accounts and share itemised transaction records (Storelink 2025). This is used by platforms like Cooklist, which allows consumers to aggregate data across accounts - including Walmart, Kroger, Safeway, Amazon, and Target, using permissioned screen scraping to automatically import purchases into a digital pantry, make recipe recommendations based on available ingredients and generate shopping lists (Storelink 2024a).

Loyalty providers are starting to set up direct data links

Evolving consumer expectations for convenience and control, and competition amongst retailers, appear to be driving loyalty providers to improve data access and the ability to more easily share data (ALA 2025). Loyalty program providers and retailers are developing features that allow users to link their accounts directly with other select services to use this data more seamlessly. For instance, Woolworths Group allows

Everyday Rewards members to link their accounts with affiliated services - such as Healthylife - to receive personalised health and nutrition insights generated from shared transaction data (Healthylife 2025).

E.2 Data access in the agricultural machinery and equipment sector

Modern farms are data intensive businesses. Tractors, harvesters, sprayers, irrigation systems and livestock tags can generate continuous streams of information on location, inputs, yields and animal movements, often feeding into cloud platforms and farm management software in near real time.

Data from farm machinery and equipment is a central part of this emerging digital system. Data from tractors and harvesters can be downloaded to analyse performance and yields or uploaded back to machines as prescription maps for seeding or spraying. As table E.3 illustrates, different types of machinery generate distinct datasets – from fuel use and operating hours through to grain moisture, bale weights or soil moisture – that can inform decisions about maintenance, input use and longer-term investment.

Table E.3 – More machines, more data and more applications

Examples of data generated by farm equipment and its potential uses

Machine / equipment type	Types of data collected	Possible applications
Tractors	Location, fuel consumption and operational hours	Maintenance decision making and investment decisions
Combine harvesters	Grain yield, moisture content, location, fuel use and operational hours	Operational decision making and production decisions
Seeders and Planters	Seeding rate, depth seed spacing and location	More accurate planting decisions
Sprayers	Droplet shape and size (application rates) and GPS coverage maps	Reducing waste and environmental regulation compliance
Irrigation systems	Water flow, pressure, soil moisture and temperature	Water efficiency, leak detection and irrigation scheduling
Drones	Vegetation coverage and temperatures	Plant health and target interventions
Soil sensors	Moisture, pH, salinity, temperature and nutrients	Target irrigation and fertilisation over time

a. This table presents the indicative data collection capabilities of some (but not all) equipment within these categories.

Sources: Agriculture Victoria (2020), Continuum Ag (2025), Huynh and Nguyen (2024), INCYT (2025), Iqbal et al (2022), Precision Ag Solutions (2025), Rejeb et al (2022), Technotron (nd).

Machinery data is only one stream in a wider farm data ecosystem that includes soil tests, satellite and drone imagery, livestock and animal health records, financial and inventory data, and information collected to meet supply-chain and regulatory requirements (figure E.2). When these datasets are integrated, they can support a wide range of decisions, including (Borthakur and Keijser 2023; Melzer et al. 2023, pp. 2, 4):

- day-to-day operations and monitoring, such as tracking livestock locations
- agronomic planning, for example by sharing yield and input data with agronomists to inform crop rotations and harvest timing

- record-keeping and compliance, such as verified records of pesticide and fertiliser applications, water use and other management activities.

The accessibility of agricultural machinery and equipment data has improved markedly …

To make full use of the data that their equipment and machinery generate, farmers need to know what is being captured and be able to access it, or share it with third parties, so it can be processed and combined with other data sources. They must also be able to upload data to their machinery (for example, specific spraying or seeding maps) and pass data between machines and different implements so that they can be used together (for example, connecting a sprayer or seeder to a tractor).

Figure E.2 – A range of data is generated and used by farmers
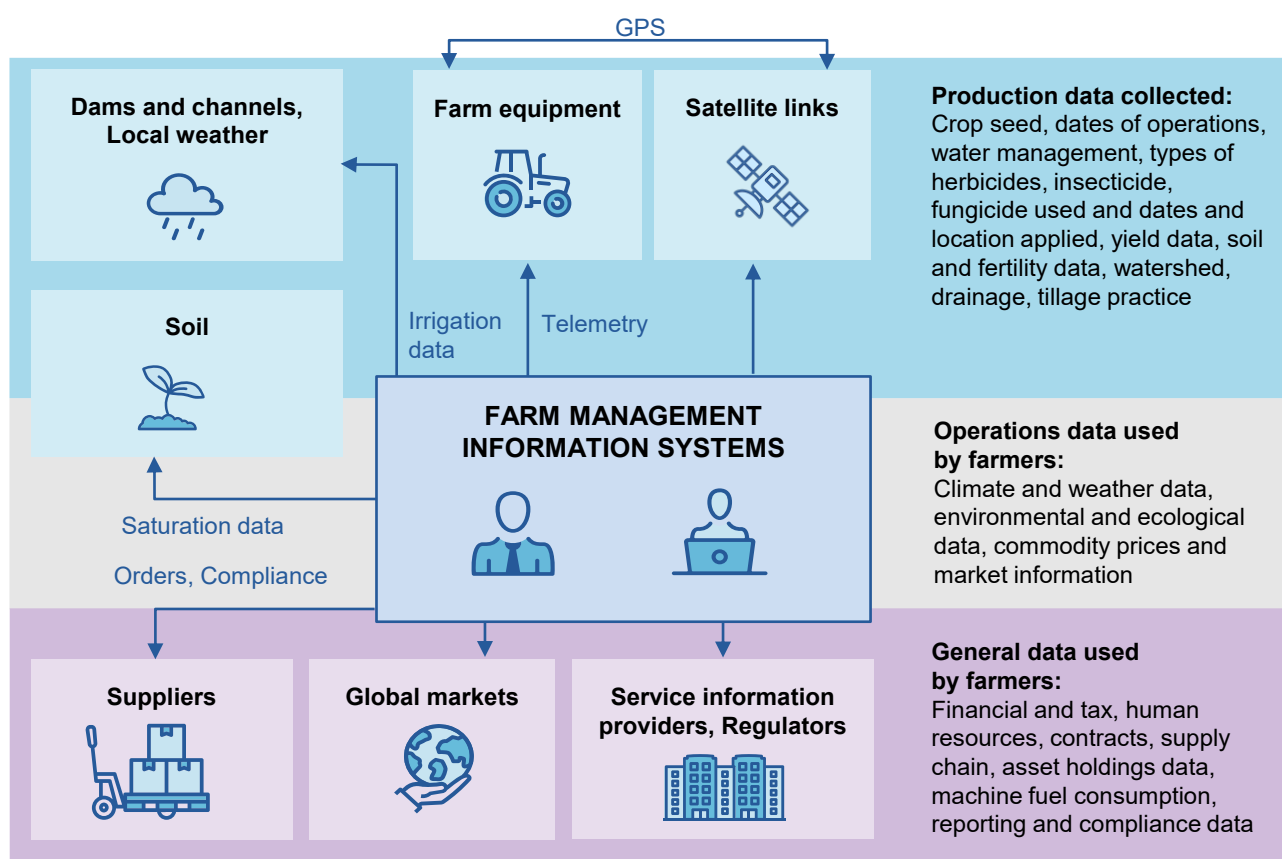
Sources: Adapted from Aspexit (2021, p. 10) and OECD (2020, p. 30).

Historically, this meant transferring data manually using USBs and SD cards, and the absence of common exchange standards often resulted in compatibility issues (Aspexit 2021, p. 10; Bewong et al. 2023, p. 40; Higgins et al. 2019, p. 72). Concerns about losing access to historical data or being unable to move it across systems meant that farmers were less inclined to switch between different brands or operate mixed fleets (Keogh and Henry 2016, p. 27; OECD 2020, p. 18).

Manufacturers now commonly pair their products with cloud-based portals that allow farmers to wirelessly send and receive machine and agronomic data, and to visualise it with built-in mapping and analytics tools. These portals often allow for automated data extraction (using APIs (Application Programming Interfaces)) that enables farmers to grant agronomists access to relevant data or connect to third-party applications. This

includes Farm Management Information Systems (FMIS), which act as digital hubs for exchanging and analysing operational, agronomic and financial data, and have evolved to help farmers manage the growing volume and complexity of farm data to better inform decision-making. For example, Agworld – a widely used Australian FMIS – allows farmers to upload machine-job data and reconcile it with budget and cost data, and agronomic records (Agworld 2025; Groeneveld 2021).

Multiple international bodies and initiatives have also emerged to develop and promote data standards for agricultural machinery (Aspexit 2021, pp. 10–15; Bahlo et al. 2019, pp. 461–462; Bewong et al. 2023, pp. 85–86). A core standard maintained through the International Organization for Standardization is 'ISOBUS' (ISO 11783), which defines a common way for tractors, on-board terminals and implements to communicate. Within this standard, the ISOXML task-data format specifies how job and machine-operation data are recorded and exchanged between equipment and farm management software (box E.1). In 2008 the Agricultural Industry Electronics Foundation (AEF) was established by major manufacturers and industry associations as a global industry body to support the implementation of these standards (AEF 2018). The AEF publishes implementation guidelines, operates conformance testing and certification, and organises regular 'Plugfest' events where companies field-test cross-compatibility (AEF nd, pp. 4, 6; AEM 2025).

Box E.1 – ISOBUS and ISOXML are two examples of common standards

Common data standards have been introduced to increase the ease with which machine data can be transformed into usable formats and shared between machines. ISOBUS and ISOXML are two examples of common data standards developed for machinery and equipment used in agriculture.

The ISOBUS (ISO 11783) standard is a communication protocol that defines how data is moved between equipment (ISO nd). Widely adopted by the industry in the 2000s, ISOBUS provides a common language to enable specific functions, such as sending the user interface for an implement to the terminal of a tractor and mapping joystick buttons (Aspexit 2021, pp. 5–6; AutoPi 2025). On newer equipment, ISOBUS also allows the implement to control certain tractor functions. For example, a round baler can stop the tractor once a bale is ready for release and can make it eject the bale. These types of integrations and functions can further simplify the work of the tractor operator.

ISOXML (ISO 11783-10) is a task-data format that sits within the ISOBUS standard to support the exchange of data between machine terminals and Farm Management Information Systems (FMIS) (Aspexit 2021). It specifies how information about field operations (such as sowing and fertilisation), products used, and machine data is structured so that different software and terminals can interpret it (Farmdok GmbH 2023). In practice, onboard terminals and FMIS software typically convert their own internal proprietary data formats to and from ISOXML for exchange (as opposed to recording data in the format) (Aspexit 2021).

As an example of how the standards work in practice, a file can be exported from an FMIS platform in ISOXML format. This file can then be loaded into an ISOBUS terminal in order to connect a tractor and a seeder. The data in ISOXML format may then be translated into a proprietary format by the seeder, which will allow it to recognise and use the data to lay seeds in a specific pattern and area (Dev 4 Agriculture 2025, p. 4; ROJ Agri-Motion nd).

...but farmers can still encounter data access issues

The PC's consultation with industry representatives indicated that most modern farm machinery and equipment will allow farmers to view and export production-related data. However, a range of technical and practical challenges can make it less than seamless when it comes to putting data to use.

Inconsistent use of flexible data standards. Widespread adoption of common data standards has made it easier to exchange farm data in a large global market (although some manufacturers continue to rely on their own proprietary formats for cost and technical reasons). Ironically the flexibility of these standards– (for example, for different naming conventions) which accommodates the diverse functionality and system architecture of different brands – can cause compatibility issues when farmers want to transfer data from one platform to another (Aspexit 2021, p. 23). And like all digital technology, the periodic updating of standards needed to keep up with the release of new product features can lead to temporary or permanent compatibility issues, requiring data to be converted back to earlier versions and limiting the functionality available in the field (Pix4D 2024; Wiebeler 2024).

Potentially too much choice in data platforms and tools. In recent years there has been a proliferation of data platforms and analytics tools to meet various demands. Munro and Geeves (2025, p. 2) observed that this can mean farmers have to juggle multiple apps, logins and data formats making it difficult 'to piece together a complete picture of the farm' and hindering decision-making, data accuracy and compliance. Research undertaken by CSIRO (2024, p. 14) for the Australian Agricultural Sustainability Framework similarly finds that data sharing in the sector relies heavily on 'point in time' or siloed solutions, resulting in a complex mix of often incompatible datasets and apps that address narrow use cases.

This fragmentation can extend beyond the farm gate. Processors, exporters, retailers, banks and certification schemes are increasingly asking producers to supply detailed information on environmental, social and governance (ESG) metrics and traceability, often through separate portals and reporting formats (CSIRO 2024, pp. 14, 20; NFF, sub. 585, p. 4; DAFF 2024). The *National Agricultural Traceability Strategy 2023–2033* notes that agribusinesses incur unnecessary costs configuring their systems to meet overlapping obligations that serve similar purposes, leading to inefficiencies and information irregularities between supply-chain partners (DAFF 2023, pp. 21, 23).

Restrictive data licensing and digital locks. Data licensing arrangements attached to farm equipment software are often complex – a problem not confined to the farm sector (chapter 4) – and their terms can be unilaterally updated by manufacturers (ACCC 2021, p. 53). Jouanjean et al (2020, p. 7) highlighted that of particular concern to farmers are clauses that prevent them from sharing data across different suppliers. Opaque licensing terms may also impede innovation – a 2023 survey found that 53% of agriculture technology businesses only 'rarely' or 'sometimes' had information on data licensing or other requirements when looking to reuse data (Bewong et al. 2023, p. 50).

Manufacturers can also restrict access to certain types of data altogether, using digital locks or encrypted interfaces (technology protection measures, or TPMs). TPMs are regularly used to control access to machine diagnostic data, preventing farmers and independent repairers from diagnosing faults and activating replacement parts. Previous reviews undertaken by the PC and the Australian Competition and Consumer Commission (ACCC) have found that OEM (original equipment manufacturer) restrictions on diagnostic data, software and tools cause material harm to farmers through higher prices, reduced choice of repairers, and longer machine downtime which can result in significant production losses (ACCC 2021, pp. 39–40; PC 2021, pp. 138, 294–296).

New tools and services have been developed to help farmers stitch machinery and equipment data together

To help deal with some of the problems discussed above, new tools and services have emerged to help farmers manage the complexity of mixed machinery fleets and bespoke analytics platforms. These solutions do not replace data standards, but sit in between machines, OEM portals, and farm management software to translate and integrate data in varied formats and across different systems.

In broad terms, translation tools convert data from one format or data model into another so that different software can interpret and use it consistently, whereas integration tools connect to multiple portals and devices and consolidate data into a single view or data feed, reducing the need for farmers to manage several logins and data export processes. A range of solutions providing one or both functions have been developed by industry bodies, OEM joint ventures and independent agriculture technology businesses (box E.2).

The availability of these types of tools means that farmers and software vendors are less dependent on manufacturers adhering to a single uniform data standard. This is particularly useful in a global market where manufacturers are regularly adding new features and functions to their products and where the domestic agricultural sectors of different countries have their own terminology. These tools nonetheless utilise baseline standards such as ISOBUS and ISOXML as an important foundation, and rely on OEMs to implement data export functionality and open interfaces so that machine data can actually be shared.

Box E.2 – Examples of data integration and translation solutions

ADAPT – a common agronomic data model and translation toolkit

ADAPT (Agricultural Data Application Programming Toolkit) is an open-source software toolkit that was developed by AgGateway, a global industry group made up of 200 member organisations from the equipment, software and data service provider sectors (AgGateway 2025a, 2025b). The tool is designed to translate agronomic task-data between proprietary machine and software formats. Rather than changing the way data is collected or stored, it makes it easier to exchange and reuse once it has been exported. To do this, OEMs (Original Equipment Manufacturers) and software vendors develop ADAPT plugins that map their proprietary file formats into the ADAPT model. Once those plugins exist, a farm management information system can support multiple brands by connecting to ADAPT rather than needing its own converters for each file type (Aspexit 2021, pp. 12, 18).

DataConnect – OEM-to-OEM integration

DataConnect is a cloud-to-cloud service jointly developed by John Deere, CLAAS, CNH Industrial and 365FarmNet. It allows farmers to see basic telematics information (such as machine location, operating status, speed and fuel level) for participating brands in a single OEM portal, without having to log into each system separately (CLAAS 2025; Claver 2020). Each OEM continues to operate its own cloud platform, but they share a small, agreed set of data fields so that mixed fleets can be viewed together (the data continues to be stored in the originating OEM systems) (Business Wire 2021; CLAAS 2025).

Third party services – such as Pairtree, Data Farming and agrirouter

Pairtree, Data Farming and agrirouter are independent organisations that provide services and tools which help farmers and agribusinesses connect, move, analyse, and use data generated by machinery, sensors, software systems, and on-farm operations (agrirouter 2025; DataFarming 2025;

> **Box E.2 – Examples of data integration and translation solutions**
>
> Pairtree 2024a). As an example, Pairtree is one private provider that provides integration tools and dashboards. Their services pull feeds from many devices, OEM portals and other third-party services – such as weather data – into farmer-configured dashboards (Pairtree 2024b). Pairtree also offers a normalised API (Application Programming Interface) for others to connect to and consume data from.

Efforts to support fairer access terms for farm data

In 2020 the National Farmers Federation (NFF) introduced the *Farm Data Code* to help address some of the contractual challenges that farmers face (Dale and Heath 2023; NFF 2023b).

The Code was developed with support from the Australian Government and input from farmers, researchers, and tech providers. It aims to promote transparency, trust, and responsible data practices in agriculture by helping farmers understand to how their data is collected, used, and shared and by providing a framework to compare service providers and inform negotiations about data policies (NFF 2023a, p. 4). It is also intended to improve the data practices of providers. For example, providers have revised their terms and conditions and data management policies to meet the Code's certification requirements (NFF, sub. 585, p. 3).

Under the Code, providers can seek certification for individual products, projects or services that handle farm data. Providers submit their terms and data management policies to the NFF for desktop assessment against the Code's principles, with applications considered by an independent certification panel. Providers that are found to comply fully can display the Code's certification logo as a trust mark and have a summary audit report published on a public register that farmers can use to compare how different tools manage their data. Although the certification scheme is still relatively new – the first products were certified in late 2023 – by late 2025 more than a dozen farm management, sensor and traceability services had been certified (NFF nd). While uptake and enforcement are known challenges for farm data codes (Wiseman et al. 2019, p. 13), the scheme has the potential to create market pressure for providers to offer better access data terms.

A right to repair framework could improve access to diagnostic data

As part of its 2021 *Right to Repair inquiry*, the PC recommended the introduction of an obligation on that would require agricultural machinery manufacturers to provide access to repair information and diagnostic-software tools (PC 2021, p. 301). The obligation would compel manufacturers to provide this access to machinery owners and independent repairers on fair and reasonable commercial terms. The ACCC has likewise recommended that agricultural machinery be considered for inclusion in the *Motor Vehicle Service and Repair Information Sharing Scheme* (box E.3).

More reliable access to diagnostic data could reduce downtime at critical periods, allow a greater share of maintenance to be carried out by independent local repairers and strengthen competitive pressure on dealer repair prices. As part of modelling of proposed competition policy reforms in 2024, the PC estimated that implementing a right to repair in the agricultural sector could increase the value of grain production alone by 3% – which equates to an increase in gross domestic product of $97M (PC 2024c, p. 90). In November 2025, the Australian Government announced that it will extend Right to Repair reforms to agricultural machinery as part of an updated *National Competition Policy Agreement* (Chalmers 2025).

Box E.3 – The MVIS could be extended to include agricultural machinery

The Motor Vehicle Service and Repair Information Sharing Scheme (MVIS) was introduced in July 2022 within the *Competition and Consumer Act 2010* (Cth) and is Australia's first right to repair law. It aims to support competition in the market for motor vehicle service and repair by requiring manufacturers to provide diagnostic, repair and service information to independent repairers at market value costs. The scheme currently only covers passenger and light goods vehicles.

Treasury completed an initial review of the scheme in December 2025 which found that it is broadly realising its legislated objectives by enhancing consumer choice, and contributing to increased productivity and competition in the automotive repair sector. While the review did not examine its potential expansion into other sectors (such as agricultural equipment), its findings are intended to inform whole-of-government efforts to develop broader right to repair reforms.

F. Recent Privacy Act reforms

A review of the *Privacy Act 1988* (Cth) was commenced in 2020, with the final report released in February 2023. The recent review made 116 recommendations to reform the Privacy Act, following three general themes (key recommendations are set out in table F.1).

Table F.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 that 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 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 Office of the Australian Information Commissioner to develop a Children's Online Privacy Code
- granting the Office of the Australian Information Commissioner 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).

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 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 F.1), 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).

Box F.1 – Concerns about the cost-benefit analysis for the Privacy Act Review

Multiple parties who had been consulted on the draft cost-benefit analysis said 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 the Australian Government to respond to these limitations may have contributed to poorly designed recommendations that place unnecessary costs on entities (ABA et al. 2024).

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 (chapter 1, box 1.4).

> 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)

One example of this is the proposal to introduce a right to erasure, modelled on the corresponding GDPR right (AGD 2023b, pp. 172, 174). In essence, this would be 'a right to have information deleted' (AGD 2023b, 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 2023b, 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).

Optus 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)

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). The overall impact of the GDPR on small to medium enterprises has been consistently noted and was specifically referred to in the European Commission's Second Report on the Application of the GDPR (European Commission 2024, pp. 13–16).

This inquiry heard support for the right to erasure from Microsoft, who is already GDPR compliant (sub. 574, p. 5) and claims to be the first company globally 'to apply consumer rights under the GDPR, including the right to erasure' (sub. 574, p. 6).

However, there were also concerns that a right to erasure could introduce significant new complexity for regulated entities. The Tech Council of Australia said:

Introducing a GDPR-style right to erasure as another piecemeal addition to the Privacy Act will create significant operational and compliance burdens. It may also lead to regulatory uncertainty where it may conflict with existing data retention obligations. (sub. 534, p. 16)

This was echoed by the Business Council of Australia:

Regarding the right to erasure, in our experience, with large and complex systems, deleting certain pieces of information can put at risk connection between records, make it harder to keep accurate histories and weaken tools that help detect fraud or cyber-attacks. (sub. 488, p. 11)

FinTech Australia expressed concern that the additional compliance burden a right to erasure would bring would have a disproportionate impact and widen the so-called '"compliance moat" that established, larger

entities have over smaller entities by virtue of the large entities' capacity to comply with technical or regulatory complex obligations' (sub. 578, p. 13).

In light of these concerns, the Productivity Commission considers that any further reforms to implement the recommendations of the Privacy Act Review – and in particular a right to erasure – 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.

Abbreviations

ABS	Australian Bureau of Statistics
ACCC	Australian Competition and Consumer Commission
ACL	Australian Consumer Law
ADAPT	Agricultural Data Application Programming Toolkit
ADR	Accredited Data Recipient
ADI	Authorised deposit-taking institution
AEF	Agricultural Industry Electronics Foundation
AI	Artificial intelligence
API	Application Programming Interface
APPs	Australian Privacy Principles
ASIC	Australian Securities and Investments Commission
ASX	Australian Securities Exchange
ATO	Australian Taxation Office
BLADE	Business Longitudinal Analysis Data Environment
CAIRG	Copyright and Artificial Intelligence Reference Group
CCA	Competition and Consumer Act 2010 (Cth)
CDR	Consumer Data Right
CSIRO	Commonwealth Scientific and Industrial Research Organisation
CSV	Comma separated values
DISR	The Department of Industry, Science and Resources'
ECL	Extended collective licensing
EDGAR	Electronic Data Gathering, Analysis and Retrieval
EU	European Union
EUR	Euro
ESG	Environmental, Social and Governance
FLOPS	Floating point operations per second
FMIS	Farm Management Information System
GDP	Gross domestic product
GDPR	General Data Protection Regulation
GPS	Global Positioning System
HTML	HyperText Markup Language

ICIP	Indigenous Cultural and Intellectual Property
ID	Identification
IFRS	International Financial Reporting Standards
IP address	Internet Protocol address
iXBRL	Inline eXtensible Business Reporting Language
JSA	Jobs and Skills Australia
LLM	Large language model
MFP	Multifactor productivity
MHR	My Health Record
MVIS	Motor Vehicle Service and Repair Information Sharing Scheme
NFF	National Farmers' Federation
OAIC	Office of the Australian Information Commissioner
OECD	Organisation for Economic Co-operation and Development
OEM	Original Equipment Manufacturer
PC	Productivity Commission
PDF	Portable Document Format
PIMSs	Personal Information Management Systems
PoS	Point of Sale
PPP	Purchasing power parity
qr	Questionnaire response
SBR	Standard Business Reporting
SD card	Secure Digital card
SMEs	Small and medium-sized enterprises
TDM	Text and data mining
TGA	Therapeutic Goods Administration
UK	United Kingdom
US	United States
USB	Universal Serial Bus
USD	United States Dollar
US SEC	United States Securities and Exchange Commission
WEF	World Economic Forum
WHS	Work Health and Safety
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, *Submission to Attorney-General's Department Privacy Act review – issues paper*.

—— 2020b, *Submission to inquiry into future directions for the Consumer Data Right*.

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, 2023-24 financial year*, www.abs.gov.au/statistics/economy/ national-accounts/australian-system-national-accounts/2023-24 (accessed 11 July 2025).

—— 2025c, *Australian system of national accounts, 2024-25 financial year*, www.abs.gov.au/statistics/economy/ national-accounts/australian-system-national-accounts/latest-release (accessed 27 November 2025).

—— 2025d, *Consumer price index, Australia, June quarter 2025*, www.abs.gov.au/statistics/economy/price-indexes-and-inflation/consumer-price-index-australia/jun-quarter-2025 (accessed 20 October 2025).

—— 2025e, *Estimates of industry multifactor productivity*, www.abs.gov.au/statistics/industry/industry-overview/estimates-industry-multifactor-productivity/2023-24 (accessed 11 July 2025).

—— 2025f, *Labour account*, www.abs.gov.au/statistics/labour/labour-accounts/labour-account-australia/mar-2025 (accessed 25 November 2025).

—— 2025g, *Privacy and legals*, www.abs.gov.au/privacy-and-legals (accessed 31 October 2025).

ACCC (Australian Competition and Consumer Commission) 2019, *Customer loyalty schemes – final report*.

—— 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, *Designated complaints legislation welcomed*, Media release, 15 February.

—— 2024c, *Digital platform services inquiry*, Interim report 8.

—— 2025a, *Accreditation guidelines – version 6*.

—— 2025b, *Supermarkets inquiry: final report*.

—— 2025c, *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*.

ACCI (Australian Chamber of Commerce and Industry) 2025, *Future of Work report unbalanced and impractical*.

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)*.

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

AEF (Agricultural Industry Electronics Foundation) 2015, *AEF: powering agricultural electronics*.

—— 2018, *2008 to 2018: AEF celebrates 10th anniversary*, www.aef-online.org/aef-news/2008-to-2018-aef-celebrates-10th-anniversary.html (accessed 27 November 2025).

—— 2025a, *About the AEF*, www.aef-online.org/about-us/about-the-aef.html#/About (accessed 25 November 2025).

—— 2025b, *Core members*, www.aef-online.org/about-us/core-members.html (accessed 25 November 2025).

—— nd, *The AEF – Ag Industry's initiative in electronic standards implementation*, www.aef-online.org/fileadmin/user_upload/Content/pdfs/AEF_Keynote_EN.pdf (accessed 3 December 2025).

AEM (Assocation of Equipment Manufacturers) 2025, *AEF fall plugfest brings manufacturers together to improve Ag equipment operability*, www.aem.org/news/aef-fall-plugfest-

brings-manufacturers-together-to-improve-ag-equipment-operability (accessed 27 November 2025).

AFIA (Australian Finance Industry Association) 2023, *Submission to discussion paper on 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) 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, *Privacy Act review report*.

AgGateway 2025a, *ADAPT: Ag data application programming toolkit*, adaptframework.org/ (accessed 1 October 2025).

—— 2025b, *Mission*, aggateway.org/AboutUs/ Mission.aspx (accessed 27 November 2025).

Aghion, P and Bunel, S 2024, *AI and growth: where do we stand*, Working paper, Federal Reserve Bank of San Francisco.

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

Agriculture Victoria 2020, *Choosing the right soil moisture monitoring device*, agriculture.vic.gov.au/farm-management/soil/choosing-the-right-soil-moisture-monitoring-device (accessed 1 December 2025).

agrirouter 2025, *Your universal solution for data exchange*, agrirouter.com/en (accessed 27 November 2025).

Agworld 2025, *Modern farm management software that works where you do*, www.agworld.com/au/products/ (accessed 14 October 2025).

Ahuja, A and Gupta, M 2024, 'Optimizing predictive maintenance with machine learning and IOT: a business strategy for reducing downtime and operational costs', *Journal of Emerging Technologies and Innovative Research*, vol. 11, no. 10, pp. 286–292.

AI CPA and XBRL International (American Institute of Certified Public 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).

ALA (Australian Loyalty Association) 2024, *ALA annual loyalty insights report*.

—— 2025, *Australia loyalty programs market report 2025*, australianloyaltyassociation.com/australia-loyalty-programs-market-report-2025/ (accessed 5 November 2025).

ALCS (Authors' Licensing and Collecting Society) 2025, *Copyright and AI: consultation response*.

Allen, W and Newton, S 2025, *Introducing pay per crawl: enabling content owners to charge AI crawlers for access*, Cloudflare, blog.cloudflare.com/introducing-pay-per-crawl/ (accessed 31 October 2025).

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*, 122.

Altman, S 2025, *Three observations*, blog.samaltman.com/three-observations (accessed 3 July 2025).

Apple Inc. 2025, *Apple Health*, www.apple.com/au/health/ (accessed 3 December 2025).

APRA AMCOS (Australasian Performing Right Association and Australasian Mechanical Copyright Owners Society and Goldmedia) 2024, *AI and music: market development of AI in the music sector and impact on music creators in Australia and New Zealand*.

ARCA (Australian Retail Credit Association) 2020, *Submission to Attorney-General's Department Privacy Act review – issues paper*.

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=VtcsAl53xAs (accessed 30 April 2025).

—— 2022, *ePayments code*.

—— 2024, *ASIC urges businesses to prepare for mandatory climate reporting*, Media release 24-205MR, 18 September.

—— 2025a, *ASIC approves Cboe's listing application to bolster competition in public markets*, Media release 25-227MR, 7 October.

—— 2025b, *Digital financial reports*, asic.gov.au/regulatory-resources/financial-reporting-and-audit/preparers-of-financial-reports/digital-financial-reports/ (accessed 27 February 2025).

—— 2025c, *Search fees*, www.asic.gov.au/for-business-and-companies/forms-and-fees/all-fees/search-fees/ (accessed 10 July 2025).

—— 2025d, *Sustainability reporting*, RG 280.

—— 2025e, *Who must prepare a sustainability report?*, www.asic.gov.au/regulatory-resources/sustainability-reporting/for-preparers-of-sustainability-reports/who-must-prepare-a-sustainability-report/ (accessed 17 November 2025).

Aspexit 2021, *Standards and data exchange in agriculture*, www.aspexit.com/standards-and-data-exchange-in-agriculture/ (accessed 4 December 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*.

—— 2025, *Test case litigation program*, www.ato.gov.au/individuals-and-families/your-tax-return/if-you-disagree-with-an-ato-decision/seek-an-external-review-of-ato-decisions/test-case-litigation-program (accessed 7 November 2025).

Australian Government 2019, *Budget Paper No. 2*, Budget Measures 2019-20.

—— 2023, *Consumer Data Right newsletter: 26 May 2023*.

—— 2024, *What is CDR? | Consumer Data Right*, www.cdr.gov.au/what-is-cdr (accessed 18 September 2024).

—— 2025a, *Become an accredited data recipient*.

—— 2025b, *CDR in the non-bank lenders sector*.

—— 2025c, *Compliance guide for data holders: Banking and non-bank lenders sectors*.

—— 2025d, *Legal obligations for data recipients*, www.cdr.gov.au/ (accessed 25 November 2025).

—— 2025e, *Rollout | Consumer Data Right*, www.cdr.gov.au/rollout (accessed 25 November 2025).

AutoPi 2025, *What is ISOBUS (ISO 11783)? A guide to tractor and agricultural equipment communications*, www.autopi.io/blog/what-is-isobus-and-iso11783/ (accessed 27 November 2025).

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.

Bahlo, C, Dahlhaus, P, Thompson, H and Trotter, M 2019, 'The role of interoperable data standards in precision livestock farming in extensive livestock systems: A review', *Computers and Electronics in Agriculture*, vol. 156, pp. 459–466.

BCA (Business Council Australia) 2024, *Inquiry into the digital transformation of workplaces, Business Council of Australia submission*.

Bengio, Y, Mindermann, S, Privitera, D, Besiroglu, T, Bommasani, R, Casper, S, Choi, Y, Fox, P, Garfinkel, B, Goldfarb, D, Heidari, H, Ho, A, Kapoor, S, Khalatbari, L, Longpre, S, Manning, S, Mavroudis, V, Mazeika, M, Michael, J, Newman, J, Ng, KY, Okolo, CT, Raji, D, Sastry, G, Seger, E, Skeadas, T, South, T, Strubell, E, Tramèr, F, Velasco, L, Wheeler, N, Acemoglu, D, Adekanmbi, O, Dalrymple, D, Dietterich, TG, Felten, EW, Fung, P, Gourinchas, P-O, Heintz, F, Hinton, G, Jennings, N, Krause, A, Leavy, S, Liang, P, Ludermir, T, Marda, V, Margetts, H, McDermid, J, Munga, J, Narayanan, A, Nelson, A, Neppel, C, Oh, A, Ramchurn, G, Russell, S, Schaake, M, Schölkopf, B, Song, D, Soto, A, Tiedrich, L, Varoquaux, G, Yao, A, Zhang, Y-Q, Albalawi, F, Alserkal, M, Ajala, O, Avrin, G, Busch, C, de Carvalho, ACP de LF, Fox, B, Gill, AS, Hatip, AH, Heikkilä, J, Jolly, G, Katzir, Z, Kitano, H, Krüger, A, Johnson, C, Khan, SM, Lee, KM, Ligot, DV, Molchanovskyi, O, Monti, A, Mwamanzi, N, Nemer, M, Oliver, N, Portillo, JRL, Ravindran, B, Rivera, RP, Riza, H, Rugege, C, Seoighe, C, Sheehan, J, Sheikh, H, Wong, D and Zeng, Y 2025, *International AI Safety Report*, arXiv, arxiv.org/abs/2501.17805 (accessed 3 December 2025).

Bergeaud, A 2024, 'The past, present and future of European productivity', presented at the *ECB Forum on Central Banking*.

Bersh, L 2024, 'An exceptional formality under Berne: evasion of copyright protection via the EU's text and data mining exception', *Harvard Journal of Law & Technology*, vol. 38, 1 Fall 2024, pp. 337–368.

Bewong, M, Ho Leung Ip, R, Lewis, C, Krivokapic-Skoko, B, Islam, MZ, Medway, J, Ali, B and Dixon, E 2023, *Potential implications and benefits for the agricultural technology sector from the introduction of the Australian Agricultural Data Exchange*, Food Agility Cooperative Research Centre.

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.

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.

Booth, R 2024, 'UK arts and media reject plan to let AI firms use copyrighted material', *The Guardian*, 20 December.

Borthakur, S and Keijser, C 2023, *Farm Management Information Systems (FMIS)*, FarmFit Insights Hub, farmfitinsightshub.org/resources/farm-management-information-systems-fmis (accessed 3 December 2025).

Bradney-George, A 2024, *Loyalty program statistics in Australia*, Finder, www.finder.com.au/credit-cards/loyalty-program-statistics (accessed 27 November 2025).

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', *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.

Bunnings 2025, *Bunnings app*, www.bunnings.com.au/campaign/bunnings-app (accessed 1 December 2025).

Business Wire 2021, *DataConnect is now available globally across six major digital platforms*, www.businesswire.com/news/home/20210701005365/en/DataConnect-Is-Now-Available-Globally-Across-Six-Major-Digital-Platforms?utm (accessed 3 December 2025).

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 (Chartered Accountants Australia and New Zealand and Wells) 2020, *The future of financial reporting: what size do you want?*

California Chamber of Commerce (Daylami) 2024, *AB 2013 (Irwin) artificial intelligence: training data transparency oppose unless amended – as amended April 22, 2024 scheduled for hearing – April 30, 2024*, Media release, 23 April.

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).

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.

CBS News 2024, 'Google strikes $60 million deal with Reddit, allowing search giant to train AI models on human posts', *CBS News*, 23 February.

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*.

Chalmers, J 2025, *Treasurers agree reforms to increase competition and boost productivity*, Treasury portfolio Media releases, ministers.treasury.gov.au/ministers/jim-chalmers-2022/media-releases/treasurers-agree-reforms-increase-competition-and-boost (accessed 1 December 2025).

Charley, S 2024, 'Physics beyond the imaginable', *Symmetry Magazine*, 9 March, www.symmetrymagazine.org/article/physics-beyond-the-imaginable?language_content_entity=und (accessed 3 December 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).

—— 2025, *How to choose the best budgeting app*, www.choice.com.au/money/financial-planning-and-investing/creating-a-budget/buying-guides/budgeting-software?utm (accessed 1 October 2025).

Chow, KW 2024, *Singapore: copyright infringement defence for AI machine learning*, Rouse, rouse.com/insights/news/2024/artificial-intelligence-in-singapore-copyright-infringement-defence-for-artificial-intelligence-machine-learning (accessed 25 November 2025).

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

CISAC (International Confederation of Societies of Authors and Composers) 2024, *Study on the economic impact of generative AI in the music and audiovisual industries*, November.

CK, V 2025, 'Qantas Frequent Flyer program's expansion sparks concerns over rising costs', *International Business Times*, www.ibtimes.com.au/qantas-frequent-flyer-programs-expansion-sparks-concerns-over-rising-costs-1855457 (accessed 4 December 2025).

CLAAS 2025, *DataConnect.*, www.claas.com/en-in/digital-solutions/data-management/data-connect (accessed 27 November 2025).

Claude 2025, *Does Anthropic crawl data from the web, and how can site owners block the crawler?*, support.claude.com/en/articles/8896518-does-anthropic-crawl-data-from-the-web-and-how-can-site-owners-block-the-crawler (accessed 11 November 2025).

Claver, H 2020, *Claas, 365FarmNet and John Deere exchange machinery data*, Future Farming, www.futurefarming.com/smart-farming/tools-data/claas-365farmnet-and-john-deere-exchange-machinery-data/ (accessed 27 November 2025).

Clifford Chance 2025, *Japan's inaugural AI regulations: a pro-innovation approach*, www.cliffordchance.com/content/dam/cliffordchance/briefings/2025/03/Japan-inaugural-ai-regulations-march-2025.pdf?utm (accessed 3 December 2025).

Cloudflare 2025a, *What is robots.txt? How a robots.txt file works*, www.cloudflare.com/learning/bots/what-is-robots-txt/ (accessed 11 November 2025).

—— 2025b, *The crawl-to-click gap: Cloudflare data on AI bots, training, and referrals*, blog.cloudflare.com/crawlers-click-ai-bots-training/ (accessed 11 November 2025).

—— 2025c, *From Googlebot to GPTBot: who's crawling your site in 2025*, blog.cloudflare.com/from-googlebot-to-gptbot-whos-crawling-your-site-in-2025/ (accessed 11 November 2025).

Coles 2025, *Switch to 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*, www.commbank.com.au/articles/newsroom/2024/11/reimagining-banking-nov24.html (accessed 3 December 2025).

—— 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*.

ContinuumAg 2025, *Harvest data collection: why it's becoming so important*, continuum.ag/harvest-data-collection-why-its-becoming-so-important/ (accessed 1 December 2025).

Cooklist 2021, *Privacy policy*, cooklist.com/privacy-policy (accessed 3 December 2025).

—— 2025, *Cooklist*, cooklist.com/ (accessed 1 October 2025).

Cormack, M 2025, *CLA announces development of generative AI training licence*, cla.co.uk/development-of-cla-generative-ai-licence/ (accessed 31 October 2025).

Council of Europe nd, *The Framework Convention on Artificial Intelligence*, www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence (accessed 1 December 2025).

Courea, E and Stacey, K 2025, 'UK ministers delay AI regulation amid plans for more "comprehensive" bill', *The Guardian*, 8 June, www.theguardian.com/technology/2025/jun/07/uk-ministers-delay-ai-regulation-amid-plans-for-more-comprehensive-bill (accessed 3 December 2025).

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

Creamer, E 2024, 'HarperCollins to allow tech firms to use its books to train AI models', *The Guardian*, 20 November.

Creative Commons 2025, *CC BY 4.0 Attribution 4.0 International*, creativecommons.org/licenses/by/4.0/ (accessed 31 October 2025).

Crunchr 2024, *The world's simplest receipt app*, crunchr.us/ (accessed 28 November 2025).

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

—— 2024, *From anarchy to order: AASF data ecosystem design project – final report*, CSIRO.

DAFF (Australian Government Department of Agriculture, Fisheries and Forestry) 2023, *National agricultural traceability strategy: 2023 to 2033*.

—— 2024, *Enhancing our world-class agricultural traceability systems*, www.agriculture.gov.au/about/news/enhancing-agricultural-traceability (accessed 4 December 2025).

Dal Molin, L, Bühler, G, Wesiak-Schmidt, K and Al Abiad, T 2025, *Swiss AI regulation: tailored rules instead of a Swiss AI Act*, Homburger, www.homburger.ch/en/insights/swiss-ai-

regulation-tailored-rules-instead-of-a-swiss-ai-act (accessed 3 December 2025).

Dale, L and Heath, NM 2023, *Farm data code update: responsible data practices in agriculture*, HWL Ebsworth Lawyers, hwlebsworth.com.au/farm-data-code-update-responsible-data-practices-in-agricultural/ (accessed 27 July 2025).

Data Standards Body 2025, *CDR Data Standards, version 1.35.1*, consumerdatastandardsaustralia.github.io/standards (accessed 1 October 2025).

DataFarming 2025, *About DataFarming*, www.datafarming.com/about (accessed 27 November 2025).

Dawson, G, Desouza, K, Denford, J and Barda Picavet, M 2025, *How different states are approaching AI*, The Brookings Institution, www.brookings.edu/articles/how-different-states-are-approaching-ai/ (accessed 3 December 2025).

Debreceny, R, Farewell, S 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*, deepmind.google/discover/blog/alphafold-a-solution-to-a-50-year-old-grand-challenge-in-biology/ (accessed 3 December 2025).

Dell 2009, *Digital information growth outpaces projections despite down economy*, www.dell.com/en-ca/dt/corporate/newsroom/announcements/2009/05/20090518-01.htm (accessed 2 December 2025).

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*, NBER working paper series no. w32146, National Bureau of Economic Research.

Department of Health and Aged Care (Australian Government Department of Health and Aged Care) 2024, *Safe and responsible artificial intelligence in health care – legislation and regulation review*.

Dev 4 Agriculture 2025, *ISOXML Libraries*, dev4agriculture.de/isoxml-library/?utm (accessed 27 November 2025).

Devlin, H 2025, 'AI to revolutionise fundamental physics and "could show how universe will end"', *The Guardian*, 3 February, www.theguardian.com/science/2025/feb/03/ai-to-revolutionise-fundamental-physics-and-could-show-how-universe-will-end (accessed 3 December 2025).

Dext 2025, *Dext for Xero*, dext.com/en/business/product/integrate-with-accounting-software/xero (accessed 28 November 2025).

DFD (Digitaliserings- og forvaltningsdepartementet [The Ministry of Digitalisation and Public Administration]) 2025, *Høring – utkast til ny lov om kunstig intelligens – gjennomføring av EUs forordning om kunstig intelligens i norsk rett*, www.regjeringen.no/no/dokumenter/3112327/id3112327/ (accessed 3 December 2025).

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).

DISR (Australian Government Department of Industry, Science and Resources) 2025a, *National AI Plan*, www.industry.gov.au/sites/default/files/2025-12/national-ai-plan.pdf (accessed 2 December 2025).

—— 2023, *The Bletchley Declaration by Countries Attending the AI Safety Summit, 1–2 November 2023*, Department of Industry, Science and Resources, www.industry.gov.au/publications/bletchley-declaration-countries-attending-ai-safety-summit-1-2-november-2023 (accessed 26 November 2025).

—— 2024a, *Voluntary AI safety standard*, National Artificial Intelligence Centre.

—— 2025b, *Australia establishes new institute to strengthen AI safety*, Department of Industry, Science and Resources, www.industry.gov.au/news/australia-establishes-new-institute-strengthen-ai-safety (accessed 26 November 2025).

—— 2024b, *Proposals paper for introducing mandatory guardrails for AI in high-risk settings*, Safe and responsible AI in Australia.

Dreyfus, M (Australian Attorney General) 2023, *Copyright and AI reference group to be established*, webarchive.nla.gov.au/awa/20231215043108/ministers.ag.gov.au/media-centre/copyright-and-ai-reference-group-be-established-05-12-2023 (accessed 19 November 2025).

DSIT (UK Department for Science, Innovation & Technology) 2024, *UK business data survey 2024*, UK Government.

DTI (Data transfer initiative) 2018, *Data Transfer Project overview and fundamentals*.

—— 2024, *The present and future of data portability*.

Duball, J 2025, '"We cannot be left behind:" How Canada is balancing AI regulation, innovation', *IAPP*, 21 May, iapp.org/news/a/we-cannot-be-left-behind-how-canada-is-balancing-ai-regulation-innovation (accessed 3 December 2025).

ekutilov 2025, *wooliesR – download eReceipts in machine-readable format*, github.com/ekutilov/wooliesR (accessed 28 November 2025).

Elkin-Koren, N and Netanel, NW 2021, 'Transplanting fair use across the globe: a case study testing the credibility of U.S. opposition', *Hastings Law Journal*, vol. 72, pp. 1121–1182.

Ellipsis 2024, *The Australia loyalty solutions market map*, www.ellipsisandco.com/blog/the-australia-loyalty-solutions-market-map (accessed 7 November 2025).

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.

EnergyFlex 2025, *EnergyFlex*, www.energyflex.com.au/ (accessed 14 July 2025).

ESMA (European Securities and Markets Authority) 2016, *Feedback statement on the consultation paper on the Regulatory Technical Standard on the European Single Electronic Format*, ESMA/2016/1668.

EU (European Union) 2025, *EU countries*, european-union.europa.eu/principles-countries-history/eu-countries_en (accessed 30 November 2025).

Europe Economics 2025, *Estimating the impact on investment of a commercial TDM exception*.

European Commission 2024, *Second report on the application of the General Data Protection Regulation*, European Commission, Brussels.

—— 2025, *Call for tenders for a feasibility study on a central registry of opt-outs under the text and data mining (TDM) exception*, digital-strategy.ec.europa.eu/en/funding/call-tenders-feasibility-study-central-registry-opt-outs-under-text-and-data-mining-tdm-exception (accessed 25 November 2025).

European Writers' Council 2025, *"A betrayal of the EU AI Act's objectives": joint statement on the GPAI Code of Practice and the template by 40 organisations*, europeanwriterscouncil.eu/ccs-joint-statement-july25/ (accessed 31 October 2025).

Everyday Rewards 2024, *Collection notice*, www.everyday.com.au/privacy/policy-documents/collection-notice.html? (accessed 1 December 2025).

—— 2025a, *Contact us*, www.everyday.com.au/contact.html (accessed 3 December 2025).

—— 2025b, *eReceipts*, www.everyday.com.au/rewards/how-it-works/ereceipts.html (accessed 28 November 2025).

—— 2025c, *Everyday extra*, www.everyday.com.au/extra.html (accessed 1 December 2025).

—— 2025d, *Managing your Everyday Rewards card*, www.everyday.com.au/support/manage-your-rewards-card.html?Everyday (accessed 1 December 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).

Eyers, J 2020, 'CBA says using fintechs exposes customers to account fraud', *Australian Financial Review*, 16 March.

Farmdok GmbH 2023, *Automatic recording with the ISOBUS display*, www.farmdok.com/en/2023/11/28/automatisch-aufzeichnen-mit-ihrem-isobus-display/ (accessed 3 December 2025).

Farquhar, S 2025, *Scott Farquhar, National Press Club Address – July 2025*, Tech Council of Australia Website, techcouncil.com.au/newsroom/scott-farquhar-national-press-club-address-july-2025/ (accessed 31 October 2025).

FCA (UK Financial Conduct Authority) 2022, *Final non-handbook guidance for firms on the Consumer Duty (FG22/5)*, FCA, London.

FDATA 2023, *Submission to discussion paper on 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, www.forbes.com.au/covers/entrepreneurs/no-more-smashed-avo-the-aussie-robot-fixing-farmings-delicate-problem/ (accessed 3 December 2025).

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, *Submission to discussion paper on screen scraping: policy and regulatory implications*.

—— 2025a, *Charting the future of the consumer data right for banking & finance*, 6th Edition.

—— 2025b, *FinTech Australia raises concerns about targeted Open Banking consultation*, Newsroom, 7 October, www.fintechaustralia.org.au/newsroom/fintech-australia-raises-concerns-about-targeted-open-banking-consultation (accessed 3 November 2025).

Fiorendino, M 2024, *Coalition Loyalty Programs Being A Driving Force for Retailers*, *CapillaryTech*, 18 October, www.capillarytech.com/blog/coalition-loyalty-programs-for-retail-brands/ (accessed 4 December 2025).

Flybuys 2025a, *Can additional cardholders on my account invite other cardholders to join?*, help.flybuys.com.au/hc/en-gb/articles/9103558612751-Can-additional-cardholders-on-my-account-invite-other-cardholders-to-join (accessed 1 December 2025).

—— 2025b, *Flybuys privacy policy*, experience.flybuys.com.au/policies/privacy-policy/?pid=pr_zendesk (accessed 1 December 2025).

—— 2025c, *How do I know who is linked to my account?*, help.flybuys.com.au/hc/en-gb/articles/9682619729295-How-do-I-know-who-is-linked-to-my-account (accessed 1 December 2025).

—— 2025d, *Velocity Frequent Flyer*, experience.flybuys.com.au/partners/velocity-frequent-flyer/ (accessed 1 December 2025).

—— 2025e, *What are my linked accounts?*, help.flybuys.com.au/hc/en-gb/articles/9682571758223-What-are-my-linked-accounts (accessed 1 December 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*, www.mcinnescooper.com/publications/the-demise-of-the-artificial-intelligence-and-data-act-aida-5-key-lessons/ (accessed 3 December 2025).

Frosio, G 2020, *Text and data mining: articles 3 and 4 of the Directive 2019/790/EU*, Center for Internet and Society at Stanford Law School, cyberlaw.stanford.edu/publications/text-and-data-mining-articles-3-and-4-directive-2019790eu/ (accessed 25 November 2025).

Gallagher, K, O'Neil, C and Mulino, D 2025, *Protecting renters and making applications easier*, Media release, 22 October, ministers.finance.gov.au/financeminister/media-release/2025/10/22/protecting-renters-and-making-applications-easier (accessed 13 November 2025).

Gantz, J 2008, *The Diverse and Exploding Digital Universe*.

—— and Reinsel, D 2012, 'The Digital Universe in 2020: Big Data, Bigger Digital Shadows, and Biggest Growth in the Far East'.

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.

Goodrich, R y A 2025, *Mexico Advances AI Governance with Landmark Legislative Proposal*, Marca Sur, marcasur.com/en/noticia/mexico-advances-ai-governance-with-landmark-legislative-proposal&f=-2025 (accessed 3 December 2025).

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

—— 2025, *How Google interprets the robots.txt specification*, developers.google.com/search/docs/crawling-indexing/robots/robots_txt (accessed 11 November 2025).

GovTech Singapore (Government of Singapore) 2025, *SGFinDex*, www.tech.gov.sg/products-and-services/for-citizens/digital-services/sgfindex/ (accessed 3 December 2025).

Grocerize 2025a, *Grocerize*, grocerize.com.au (accessed 7 November 2025).

—— 2025b, *Grocerize push to cart*, chromewebstore.google.com/detail/grocerize-push-to-cart/bbichloclklkjgochlcnkmmcigjeejmd?hl=en&pli=1 (accessed 3 December 2025).

—— 2025c, *Press release: you'd be shocked what you're overpaying for: the surprising price of complacency*, Get the Word Out, getthewordout.com.au/press-release/press-release-youd-be-shocked-what-youre-overpaying-for-the-surprising-price-of-complacency/ (accessed 7 November 2025).

Groeneveld, R 2021, *Agworld: crossing the hurdle of combining data*, Future Farming, www.futurefarming.com/smart-farming/tools-data/agworld-crossing-the-hurdle-of-combining-data/ (accessed 3 December 2025).

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

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 no. 3, Columbia Business School Center for Excellence in Accounting and Security Analysis.

Hays, S 2024, *AI training and copyright infringement: solutions from Asia*, Tech Policy, www.techpolicy.press/ai-training-and-copyright-infringement-solutions-from-asia/ (accessed 25 November 2025).

Healthylife 2025, *Healthylife x Woolworths*, www.healthylife.com.au/woolworths (accessed 7 November 2025).

Helios Salinger 2022, *Privacy Act reforms*, www.salingerprivacy.com.au/privacy-reforms/ (accessed 12 March 2025).

—— 2025, *Privacy pulse 2025: measuring maturity*.

Higgins, S, Schellberg, J and Bailey, JS 2019, 'Improving productivity and increasing the efficiency of soil nutrient management on grassland farms in the UK and Ireland using precision agriculture technology', *European Journal of Agronomy*, vol. 106, pp. 67–74.

Hilbert, M and López, P 2011, 'The World's Technological Capacity to Store, Communicate, and Compute Information', American Association for the Advancement of Science, *Science*, vol. 332, no. 6025, pp. 60–65.

Hoitash, R, Hoitash, U and Morris, L 2020, 'eXtensible business reporting language (XBRL): a review and implications for future research', *Auditing: A Journal of Practice & Theory*, vol. 40, no. 2, pp. 107–132.

Hollander, S and Litjens, R 2022, *Localised information acquisition*, SSRN 3691111.

Horn, A 2004, 'Creators and the copyright balance: investigating the interests of copyright holders, users and creators', *Alternative Law Journal*, vol. 29, no. 3, pp. 112–116.

Huynh, N and Nguyen, K-D 2024, 'Real-time droplet detection for agricultural spraying systems: a deep learning approach', *Machine Learning and Knowledge Extraction*, vol. 6, no. 1, pp. 259–282.

iapp 2025, *Global AI Law and Policy Tracker*, iapp.org/resources/article/global-ai-legislation-tracker/?utm (accessed 3 December 2025).

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*.

ICA (Insurance Council of Australia) 2020, *Submission to Attorney-General's Department Privacy Act review – issues 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*.

INCYT 2025, *Monitor and control on-farm water and irrigation assets*, www.incyt.com.au/solutions/water-and-irrigation-management?srsltid=AfmBOorFWQt-IJSuGsPNYjcjQlc6zThiMHNRwLGG9giqRz84tetsdEm- (accessed 1 December 2025).

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

Ingham, T 2025, 'Eleven Music, new AI rival to Suno, launches with Kobalt, Merlin deals – and warnings for users who want to infringe copyrights', *Music Business Worldwide*, 5 August.

IP Australia 2025, *Australian IP report 2025*.

Iqbal, T, Ghaffar, AM, ur Rehman, U, Saeed, Y, Aqib, M, Iqbal, F and Saleem, SR 2022, 'Development of real time seed depth control system for seeders', presented at International Precision Agriculture Pakistan Conference, Pakistan, 28 November.

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, theconversation.com/i-was-a-beta-tester-for-the-nobel-prize-winning-alphafold-ai-its-going-to-revolutionise-health-research-241084 (accessed 3 December 2025).

ISO (International Organization for Standardization) nd, *ISO 11783-1:2017(en) Tractors and machinery for agriculture and forestry — serial control and communications data network — part 1: General standard for mobile data communication*, www.iso.org/obp/ui?utm#iso:std:iso:11783:-1:ed-2:v1:en (accessed 12 November 2025).

ITI (Information Technology Industry Council) 2020, *Submission to Attorney-General's Department Privacy Act review – issues paper*.

Jackson, A 2025, *IEA launches observatory for data centre sustainability push*, Data Centre Magazine, datacentremagazine.com/critical-environments/all-you-need-to-know-about-ieas-energy-ai-observatory (accessed 25 November 2025).

Janssen, R, Kesler, R, Kummer, ME and Waldfogel, J 2022, *GDPR and the lost generation of innovative apps*.

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).

—— 2024c, 'The importance of trust in the modern economy', ministers.treasury.gov.au/ministers/stephen-jones-2022/speeches/address-intersekt-fintech-festival (accessed 28 November 2025).

—— 2025, *Consumer Data Right expansion to deliver a better deal for consumers*.

JSA (Jobs and Skills Australia) 2025a, *Our gen AI transition: exposures, adaptation, dynamism*, www.jobsandskills.gov.au/studies/generative-artificial-intelligence-capacity-study/occupation-data-on-ai-exposure (accessed 10 November 2025).

—— 2025b, *Our gen AI transition: final overarching report*.

Keogh, M and Henry, M 2016, *The implications of digital agriculture and big data for Australian agriculture*, Australian Farm Institute, Sydney.

Koski, H and Valmari, N 2020, *Short-term impacts of the GDPR on firm performance*, ETLA Working Papers.

Kosterit, SD 2025, *AI policy corner: the Turkish artificial intelligence law proposal*, montrealethics.ai/ai-policy-corner-the-turkish-artificial-intelligence-law-proposal/ (accessed 3 December 2025).

Kowal, E 2025, 'AI is in every NSW public school classroom. Is that a good thing?', *The Age*, 21 June, www.theage.com.au/politics/nsw/ai-is-in-every-nsw-public-school-classroom-is-that-a-good-thing-20250603-p5m4ml.html (accessed 3 December 2025).

Kyriakopoulos, V 2023, *Guide to the Everyday Rewards app*, *Point Hacks*, www.pointhacks.com.au/everyday-rewards/app/ (accessed 1 December 2025).

Langehennig, S 2025, 'Colorado is pumping the brakes on first-of-its-kind AI regulation to find a practical path forward', *The Conversation*, 22 November, theconversation.com/colorado-is-pumping-the-brakes-on-first-of-its-kind-ai-regulation-to-find-a-practical-path-forward-269065 (accessed 3 December 2025).

Lateral Economics 2014, *Open for business: how open data can help achieve the G20 growth target*, Omidyar Network.

—— 2019, *Valuing the Australian Census*.

Legal Information Institute 2025, *Binding precedent*, Cornell Law School, www.law.cornell.edu/wex/binding_precedent (accessed 24 November 2025).

Lenovo 2024, *What are floating-point operations per second (FLOPS)?*, www.lenovo.com/au/en/glossary/flops/ (accessed 1 June 2025).

Levi, S and Ghaemmaghami, M 2025, *Copyright Office weighs in on AI training and fair use*, Skadden, Arps, Slate, Meagher & Flom LLP and Affiliates, www.skadden.com/insights/publications/2025/05/copyright-office-report (accessed 25 November 2025).

——, Ridgway, W, Simon, D, Slawe, M and Oh, A 2024, *Utah becomes first state to enact AI-centric consumer protection law*, www.skadden.com/insights/publications/2024/04/utah-becomes-first-state (accessed 3 December 2025).

Li, OZ, Ni, C and Lin, Y 2012, 'Does XBRL adoption reduce the cost of equity capital?', *Available at SSRN 2131001*.

Library of Congress 2025, *Regulating artificial intelligence: U.S. and international approaches and considerations for Congress*, 4 June, www.congress.gov/crs-product/R48555?utm (accessed 3 December 2025).

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).

Loyalty & Reward Co 2019, *Australian loyalty schemes: a Loyalty & Reward Co report for the ACCC*.

Loyalty Pacific Pty Ltd 2024, *Submission on ACCC supermarket inquiry issues paper*.

Lucchi, N 2025, *Generative AI and copyright: training, creation, regulation*, Policy Department for Justice, Civil Liberties and Institutional Affairs, European Union.

Marr, B 2023, 'A short history of ChatGPT: how we got to where we are today', *Forbes*, 19 May.

Martinez, A 2025, 'New Texas AI Law Spares Employers Sweeping Rules', *Forbes*, 11 July.

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 & Company 2023, *Introducing the Australian Consumer Loyalty Survey*, www.mckinsey.com/industries/retail/our-insights/introducing-the-australian-consumer-loyalty-survey (accessed 7 November 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*.

Meley, C 2025, 'Academic publishers sign AI deals as US cuts research grants', *Bloomberg*, 11 June.

Melzer, M, Bellingrath-Kimura, S and Gandorfer, M 2023, 'Commercial farm management information systems – A demand-oriented analysis of functions in practical use', *Smart Agricultural Technology*, vol. 4, p. 100203.

Meta Platforms 2023a, *Notice of inquiry on artificial intelligence & copyright: comments of Meta Platforms, Inc*.

—— 2023b, *Notice of inquiry on artificial intelligence & copyright: reply comments of Meta Platforms, Inc*.

MFAA (Mortgage and Finance Association of Australia) 2025, *Targeted consultation – introducing a de minimis threshold for banks in the Consumer Data Right*, Submission, www.mfaa.com.au/wp-content/uploads/2025/10/20102025_MFAA-submission-to-Treasury_CDR-de-minimis-threshold.pdf (accessed 30 October 2025).

Milmo, D 2023, 'ChatGPT reaches 100 million users two months after launch', *The Guardian*, 3 February, www.theguardian.com/technology/2023/feb/02/chatgpt-100-million-users-open-ai-fastest-growing-app (accessed 3 December 2025).

MinCiencia nd, *Proyecto de Ley que Regula los Sistemas de IA*, minciencia.gob.cl/areas/inteligencia-artificial/Inteligencia-Artificial/Proyecto-Ley-regula-sistemas-IA/?utm (accessed 30 November 2025).

MinCiencias 2025, *Protecto de Ley 'Por medio del cual se regula la inteligencia artificial en Colombia para garantizar su desarrollo ético y responsable y se dictan otras disposiciones'*, 7 May, especiales.minciencias.gov.co/wp-content/uploads/2025/07/pl_ia_finalizado.pdf?utm (accessed 3 December 2025).

Ministry of Business, Innovation and Employment (NZ) 2025, *New Zealand's Strategy for Artificial Intelligence: Investing with confidence*, Ministry of Business, Innovation and Employment (MBIE) Hīkina Whakatutuki – Lifting to make successful.

Ministry of Digitalisation and Public Governance (Norway) 2025, *Paving the way for safe and innovative use of AI in Norway*, 26 March, www.regjeringen.no/en/whats-new/gjor-norge-klar-for-trygg-og-innovativ-ki-bruk/id3093081/?utm (accessed 3 December 2025).

Ministry of Science and ICT (South Korea) 2024, *A New Chapter in the Age of AI: Basic Act on AI Passed at the National Assembly's Plenary Session*, www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=4&mPid=2&bbsSeqNo=42&nttSeqNo=1071 (accessed 4 December 2025).

Misch, F, Park, B, Pizzinelli, Carlo and Sher, G 2025, *Artificial intelligence and productivity in Europe*, 67, IMF Working Papers 2025, International Monetary Fund.

Morrison Foerster nd, *Costa Rica*, www.mofo.com/artificial-intelligence/costa-rica?utm (accessed 1 December 2025).

MSCI Institute 2025, *When old tech beats new tech: sustainability reporting with XBRL*, www.msci-institute.com/themes/risk-return/when-old-tech-beats-new-tech-sustainability-reporting-with-xbrl/ (accessed 21 October 2025).

Munro, H and Geeves, C 2025, *Securing 200 more seasons: active farm management and digital integration in broadacre cropping*, Grains Research & Development Corporation.

MYOB 2025, *Solo by MYOB invoice & expense – Google Play*, play.google.com/store/apps/details?id=com.myob.solo.android&hl=en_US (accessed 4 December 2025).

NAIC (National Artificial Intelligence Centre) 2025, *AI adoption in Australian businesses for 2024 Q4*.

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.

NAVA (National Association of Voice Actors) 2025, *The state of voiceover: 2025 voiceover survey*, navavoices.org/voiceover-survey-2025/voiceover-survey-2025-part-3-ai/ (accessed 31 October 2025).

News Corp 2024, *News Corp and OpenAI sign landmark multi-year global partnership*, investors.newscorp.com/news-releases/news-release-details/news-corp-and-openai-sign-landmark-multi-year-global-partnership (accessed 20 November 2025).

News Service Bund 2025a, *Switzerland signs Council of Europe Convention on Artificial Intelligence*, www.news.admin.ch/en/nsb?id=104646&utm (accessed 3 December 2025).

—— 2025b, *Update – Current data protection legislation is directly applicable to AI*, www.edoeb.admin.ch/en/update-current-legislation-directly-applicable-ai?utm (accessed 3 December 2025).

NFF (National Farmers' Federation) 2023a, *Farm data code*.

—— 2023b, *Farm data code edition 2*.

—— 2025, *National Small Business Strategy backs agricultural right to repair*, Media release, 3 February.

—— nd, *Register of Providers*, nff.org.au/programs/australian-farm-data-code/assessment-and-certification/register-of-providers/ (accessed 3 December 2025).

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.

OAIC (Office of the Australian Information Commissioner) 2019, *Chapter 12: APP 12 Access to personal information*.

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

—— 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).

—— 2025a, *Consumer consent, authorisation and dashboards*, www.oaic.gov.au/consumer-data-right/consumer-data-right-guidance-for-business/privacy-obligations/consumer-consent,-authorisation-and-dashboards (accessed 1 December 2025).

—— 2025b, *Consumer Data Right privacy safeguards*.

OBD2 Australia 2025, *OBD2 Australia*, obd2australia.com.au/shop/ (accessed 25 November 2025).

OECD (Organisation for Economic Co-operation and Development) 2005, *OECD Guiding Principles for Regulatory Quality and Performance*.

—— 2019, *Enhancing access to and sharing of data: reconciling risks and benefits for data re-use across societies*, Paris.

—— 2020, *Issues around data governance in the digital transformation of agriculture: the farmers' perspective*, OECD Food, Agriculture and Fisheries Papers no. 146.

—— 2021, *Data portability, interoperability and digital platform competition*, Paris.

—— 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.

—— 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.

Office for the Arts 2025, *Protecting Indigenous Cultural and Intellectual Property*, www.arts.gov.au/what-we-do/indigenous-arts-and-languages/protecting-indigenous-cultural-and-intellectual-property (accessed 11 November 2025).

Olliver, A, Schlingmann, N and Van Der Vlugt, P 2023, 'ISOBUS Technologies – The Standard for Smart Agriculture', in Zhang, Q (ed), *Encyclopedia of Smart Agriculture Technologies*, Springer International Publishing, Cham, pp. 1–18, link.springer.com/10.1007/978-3-030-89123-7_117-2 (accessed 27 November 2025).

O'Mahoney, J, Berry, C, Herbert, V, Subramanian, A, Chan, A, Hull, N and Wong, B 2022, *Demystifying data*, Deloitte Access Economics.

Open Banking 2025, *Adoption analysis: open banking penetration*.

Open Finance ANZ 2025, *Australian open banking ecosystem map and report 5th Edition – January 2025*.

OpenAI 2024a, *API partnership with Stack Overflow*, openai.com/index/api-partnership-with-stack-overflow/ (accessed 20 November 2025).

—— 2024b, *Strategic content partnership with TIME*, openai.com/index/strategic-content-partnership-with-time/ (accessed 20 November 2025).

—— 2025a, *AI in Australia: OpenAI's economic blueprint*.

—— 2025b, *Buy it in ChatGPT: instant checkout and the agentic commerce protocol*, openai.com/index/buy-it-in-chatgpt/ (accessed 26 November 2025).

—— 2025c, *ChatGPT pricing*, openai.com/chatgpt/pricing (accessed 4 July 2025).

—— 2025d, *Overview of OpenAI crawlers*, platform.openai.com/docs/bots (accessed 11 November 2025).

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

Or-Hof, D 2024, *Proactive caution: Israel's approach to AI regulation*, iapp, iapp.org/news/a/proactive-caution-israels-approach-to-ai-regulation (accessed 3 December 2025).

Page, R 2021, *What are loyalty schemes like Flybuys and Everyday Rewards doing with your data?*, www.choice.com.au/data-protection-and-privacy/data-collection-and-use/who-has-your-data/articles/loyalty-program-data-collection? (accessed 1 December 2025).

Pairtree 2024a, *Pairtree*, pairtree.co/ (accessed 27 November 2025).

—— 2024b, *Pairtree Plus farm dashboard*, pairtree.co/farm-data-plus/ (accessed 25 November 2025).

Parliament of Australia 2024, *Privacy and Other Legislation Amendment Bill 2024*, parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r7249_aspassed/toc_pdf/24115b01.pdf (accessed 17 February 2025).

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.

—— 2021, *Right to Repair*, Report no. 97, Canberra.

—— 2022, *Aboriginal and Torres Strait Islander visual arts and crafts*, Study report, Canberra.

—— 2023a, *5-year Productivity Inquiry: Advancing Prosperity*, Inquiry report no. 100, 1, Canberra.

—— 2023b, *5-year Productivity inquiry: Australia's data and digital dividend*, Inquiry report no. 100, 4, Canberra.

—— 2023c, *5-year productivity Inquiry: keys to growth*, Inquiry report no. 100, 2, Canberra.

—— 2024a, *Leveraging digital technology in healthcare*.

—— 2024b, *Making the most of the AI opportunity: the challenges of regulating AI*, Research paper, no. 2, Canberra.

—— 2024c, *National Competition Policy: modelling proposed reforms*, Study report, Canberra.

—— 2025a, *Building a skilled and adaptable workforce*, Inquiry report no. 110, Canberra.

—— 2025b, *Creating a more dynamic and resilient economy*, Inquiry report no. 109, Canberra.

—— 2025c, *Harnessing data and digital technology*, Interim report, August.

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.

Pilz, KF, Rahman, R, Sanders, J and Heim, L 2025, *GPU clusters*, Epoch, epoch.ai/data/gpu-clusters (accessed 25 November 2025).

Pineda, J 2025, *Website crawling: the key to search engine visibility and indexing*, Agile Digital Agency,

www.agiledigitalagency.com/blog/website-crawling/ (accessed 11 November 2025).

Pix4D 2024, *ISOXML 3 Support*, community.pix4d.com/t/isoxml-3-support/30008 (accessed 27 November 2025).

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*.

Precision Ag Services 2025, *Understanding drone data for better farm decisions*, precisionagservices.com.au/understanding-drone-data-farm-decisions/ (accessed 1 December 2025).

PropertyMe 2025, *PropertyMe selected to pilot Federal Government-led initiative to protect renters' information*, *PropertyMe*, www.propertyme.com.au/blog/propertyme-selected-to-pilot-federal-government-led-initiative-to-protect-renters-information (accessed 13 November 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 2024, *Qantas Annual Report 2024*, Sydney.

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).

Reboot Online 2025, *Website statistics report 2025*, www.rebootonline.com/website-statistics (accessed 31 October 2025).

ReceiptJar 2025, *Turn your receipts into cash!*, www.receiptjar.com (accessed 28 November 2025).

Reconciliation Australia and Terri Janke and Company 2025, *Respecting and protecting Indigenous Cultural and Intellectual Property (ICIP)*.

Reddit 2025, *Reddit user agreement*, redditinc.com/policies/user-agreement (accessed 31 October 2025).

Reinsel, D 2007, 'The Expanding Digital Universe: Can we Contain it?', IDC Analyze the Future.

Rejeb, A, Abdollahi, A, Rejeb, K and Treiblmaier, H 2022, 'Drones in agriculture: A review and bibliometric analysis', *Computers and Electronics in Agriculture*, vol. 198, linkinghub.elsevier.com/retrieve/pii/S0168169922003349 (accessed 1 December 2025).

Richards, S 2023, 'Artificial intelligence helps catalogue Aboriginal rock art in Far North Queensland', *ABC News*, 15 September, www.abc.net.au/news/2023-09-15/artificial-intelligence-rock-art-far-north-queensland-indigenous/102851802 (accessed 3 December 2025).

Riddle, R 2024, *Frugal Newcastle dad helping shoppers save with Grocerize*, Newcastle Weekly, 12 April, newcastleweekly.com.au/newcastle-dad-creates-grocerize/ (accessed 28 November 2025).

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

ROJ Agri-Motion nd, *What is an ISOBUS system and how it works*, www.agri-motion.com/en/news/posts/what-is-an-isobus-system-and-how-it-works?utm (accessed 3 December 2025).

Rowland, M (Australian Attorney General) 2024, *New Duty of Care obligations on platforms will keep Australians safer online*, Media release, 14 November, Department of Infrastructure, Transport, Regional Development, Communications and the Arts.

—— 2025, *Albanese Government to ensure Australia is prepared for future copyright challenges emerging from AI*, Media release, 26 October.

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).

Samsung 2024, *Samsung introduces AI Family HubTM French Door Refrigerator – the latest in the home appliance lineup featuring enhanced connectivity and AI capabilities*, news.samsung.com/au/samsung-introduces-ai-family-hubtm-french-door-refrigerator-the-latest-in-the-home-appliance-lineup-featuring-enhanced-connectivity-and-ai-capabilities (accessed 28 November 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*.

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).

Shutterstock 2023, *Shutterstock expands long-standing relationship with Meta*, investor.shutterstock.com/news-releases/news-release-details/shutterstock-expands-long-standing-relationship-meta (accessed 20 November 2025).

Similarweb 2025, *GenAI and how it's impacting US publishers*.

Singapore Ministry of Law 2021, *Second reading speech by Second Minister for Law, Mr Edwin Tong SC, on Copyright Bill*.

Singer, S and Phillips-Robins, A 2025, 'California Just Passed the First U.S. Frontier AI Law. Here's What It Does.', *Emissary*, 16 October, carnegieendowment.org/emissary/2025/10/california-sb-53-frontier-ai-law-what-it-does?lang=en (accessed 3 December 2025).

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.

Smith, P 2025, 'OpenAI deal shows the value of journalism to AI giants', *Australian Financial Review*, 17 January.

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.

SoA (Society of Authors) 2024, *SoA survey reveals a third of translators and quarter of illustrators losing work to AI*, societyofauthors.org/2024/04/11/soa-survey-reveals-a-third-of-translators-and-quarter-of-illustrators-losing-work-to-ai/ (accessed 31 October 2025).

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 (Standford University Human-Centred Artificial Intelligence) 2025, *Artificial Intelligence Index report 2025*.

Storelink 2024a, *Case Study: Cooklist*, www.storelink.ai/case-studies/cooklist (accessed 1 November 2025).

—— 2024b, *User Policy*, www.storelink.ai/user-policy (accessed 3 December 2025).

—— 2025, *Storelink – SDK*, www.storelink.ai/sdk (accessed 4 December 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*.

Taylor, P 2025, *Data growth worldwide 2029*, IDC Global Datasphere Forecast, www.statista.com/statistics/871513/worldwide-data-created/ (accessed 2 December 2025).

Technotron nd, *Agricultural machinery telematics*, jv-technoton.com/solutions/agricultural-machinery-telematics/?utm (accessed 1 December 2025).

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).

Terri Janke and Company 2025, *Guide – respecting and protecting Indigenous Cultural and Intellectual Property (ICIP)*, Reconciliation Australia.

TGA (Therapeutic Goods Administration) 2024, *TGA consultation: Clarifying and strengthening the regulation of Artificial Intelligence (AI)*.

—— 2025a, *Clarifying and strengthening the regulation of medical device software including artificial intelligence (AI)*.

—— 2025b, *Legislative review report: Clarifying and strengthening the regulation of AI*.

The Point of Loyalty 2025, *For love or money 2025 – executive summary*.

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*.

Thorpe, D 2025, *4 strategic location factors for AI training data centres*, JLL, www.jll.com/en-uk/insights/four-strategic-location-factors-for-ai-training-data-centres (accessed 25 November 2025).

Tong, A, Wang, E and Coulter, M 2024, 'Exclusive: Reddit in AI content licensing deal with Google', *Reuters*, 22 February.

Treasury (Australian Government Treasury) 2018a, *Reducing the financial reporting burden for SMEs*, treasury.gov.au/small-business/frt/factsheet (accessed 27 March 2025).

—— 2018b, *Modernising business registers program – review of registry fees – consultation paper*.

—— 2021, *Consumer data right: telecommunications sectoral assessment: final report*.

—— 2022a, *Consumer Data Right – strategic assessment outcomes*.

—— 2022b, *Statutory review of the Consumer Data Right report*.

—— 2023a, *Consumer Data Right compliance costs review*, treasury.gov.au/sites/default/files/2024-08/p2024-512569-report.pdf (accessed 27 November 2025).

—— 2023b, *Screen scraping – policy and regulatory implications*, Discussion paper.

—— 2023c, *Climate-related financial disclosure – consultation paper*.

—— 2024a, *CDR rules: consent and operational enhancement amendments*, Consultation paper.

—— 2024b, *Review of tax regulator secrecy exceptions*, Consultation paper.

—— 2025a, *Consumer Data Right*, treasury.gov.au/policy-topics/economy/consumer-data-right (accessed 1 July 2025).

—— 2025b, *Pro-competition market enabling infrastructure: CDR as a case study*.

—— 2025c, *Review of AI and the Australian Consumer Law*.

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.

Tweney, D 2018, 'Here Comes the Zettabyte Age', *Wired*, www.wired.com/2010/04/here-comes-the-zettabyte-age/ (accessed 2 December 2025).

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 2024a, *Copyright and artificial intelligence*, December.

—— 2024b, *Copyright and artificial intelligence*, www.gov.uk/government/consultations/copyright-and-artificial-intelligence/copyright-and-artificial-intelligence#copyright-and-ai-consultation (accessed 3 November 2025).

UK Intellectual Property Office and Younger, JEG 2014, *New exceptions to copyright reflect digital age*, Media release, 1 June.

US Bureau of Economic Analysis 2025, *Gross Domestic Product by State and Personal Income by State, 2nd quarter 2025 and Personal Consumption Expenditures by State, 2024*, www.bea.gov/data/gdp/gdp-state (accessed 3 December 2025).

US Census Bureau 2024, *State Population Totals and Components of Change: 2020-2024*, www.census.gov/data/tables/time-series/demo/popest/2020s-state-total.html (accessed 3 December 2025).

US Copyright Office 2025a, *Copyright and artificial intelligence – part 3: generative AI training*.

—— 2025b, *U.S. Copyright Office fair use index*, www.copyright.gov/fair-use/ (accessed 12 November 2025).

US SEC (United States Securities and Exchange Commission) 2009, *Final rule: interactive data to improve financial reporting*.

—— 2024, *IFRS taxonomy*, www.sec.gov/data-research/standard-taxonomies/ifrs-taxonomy (accessed 10 July 2025).

—— 2025, *EDGAR XBRL validation errors*, www.sec.gov/data-research/xbrl-validation-rendering/edgar-xbrl-validation-errors (accessed 21 May 2025).

Virgin Australia 2025, *Velocity delivers more for members on Virgin Australia's new long haul international flights*, www.virginaustralia.com/au/en/newsroom/2025/4/velocity-delivers-more-for-members-on-virgin-australias-new-long-haul-international-flights/ (accessed 27 November 2025).

VLRC (Victorian Law Reform Commission) 2002, *Defining privacy*.

VTHC (Victorian Trades Hall Council) 2025, *Submission to the Select Committee on Adopting Artificial Intelligence*.

Walmart 2025, *Walmart partners with OpenAI to create AI-first shopping experiences*, corporate.walmart.com/news/2025/10/14/walmart-partners-with-openai-to-create-ai-first-shopping-experiences (accessed 26 November 2025).

Wang, B, Weng, L, Wu, Q and Xu, EX 2024, *Do machine-readable disclosures facilitate regulatory scrutiny? Evidence from SEC comment letters*, SSRN 4989482.

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 2025, *WeMoney*, www.wemoney.com.au/ (accessed 14 July 2025).

Wesfarmers 2025, *Wesfarmers Group data and digital and other activities*, www.wesfarmers.com.au/our-businesses/other-businesses (accessed 27 November 2025).

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*, www.westpac.com.au/news/making-news/2025/05/westpac-deploys-real-time-AI-to-take-on-scammers/ (accessed 3 December 2025).

White Label Loyalty 2024, *Top loyalty programs in Australia: a comprehensive guide*, whitelabel-loyalty.com/blog/loyalty/top-loyalty-programs-in-australia-a-comprehensive-guide (accessed 3 December 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.

Wiebeler, F 2024, *Terminal says "no" – first aid for ISOXML imports*, Dev 4 Agriculture, dev4agriculture.de/terminal-says-no-first-aid-for-isoxml-imports/ (accessed 27 November 2025).

Wiggers, K 2024, *Stack Overflow signs deal with OpenAI to supply data to its models*, TechCrunch, techcrunch.com/2024/05/06/stack-overflow-signs-deal-with-openai-to-supply-data-to-its-models/ (accessed 10 November 2025).

WiseList 2025a, *Transform your kitchen with WiseList's AI meal planner*, www.wiselist.app/ai-meal-planner/ (accessed 28 November 2025).

—— 2025b, *WiseList: grocery comparison*, www.wiselist.app/grocery-price-comparison-australia/ (accessed 26 November 2025).

—— 2025c, *Your smart pantry & fridge organiser*, www.wiselist.app/pantry-fridge-organiser/ (accessed 28 November 2025).

Wiseman, L, Pesce, V, Zampati, F, Sullivan, S, Addison, C and Drolet, J 2019, *Review of codes of conduct, voluntary guidelines and principles relevant for farm data sharing*, Technical Centre for Agricultural and Rural Cooperation.

Wolford, B 2019, *What is GDPR, the EU's new data protection law?*, gdpr.eu/what-is-gdpr/ (accessed 4 June 2025).

Woolworths Group 2024, *ASX Announcement*, www.woolworthsgroup.com.au/content/dam/wwg/investors/asx-announcements/2024/Woolworths%20Group%20F24%20Profit%20Announcement.pdf (accessed 4 December 2025).

—— 2025a, *Managing your information*, www.woolworthsgroup.com.au/au/en/privacy/managing-your-information.html (accessed 1 December 2025).

—— 2025b, *Request for access to personal information*, www.woolworthsgroup.com.au/content/dam/wwg/privacy/Request_for_Access_to_Personal-Information.pdf (accessed 4 December 2025).

—— 2025c, *Woolworths Group privacy policy*, www.woolworthsgroup.com.au/content/dam/wwg/documents/privacy/Woolworths_Group_Privacy_Policy_6%20March2025%20_3.pdf (accessed 4 December 2025).

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 2024a, *GDP, PPP (current international $) – OECD members*, data.worldbank.org/indicator/NY.GDP.MKTP.PP.CD?locations=OE (accessed 3 December 2025).

—— 2024b, *Population, total – OECD members*, data.worldbank.org/indicator/SP.POP.TOTL?locations=OE (accessed 3 December 2025).

—— 2025, *PPP conversion factor, Australia*, data.worldbank.org/indicator/PA.NUS.PPP?locations=AU (accessed 30 June 2025).

X 2024, *Terms of service*, x.com/en/tos (accessed 10 November 2025).

XBRL International 2013, *Using XBRL data aggregator's perspective – XBRL best practices board data consumption webinar series [video]*, YouTube, www.youtube.com/watch?v=7pOMQ_7Gne8 (accessed 20 October 2025).

—— 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 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 2024, *Claim expenses instantly: Xero's receipt scanner app*, www.xero.com/au/accounting-software/claim-expenses/scan-receipts/ (accessed 28 November 2025).

Youtube 2024, *Third party AI trainability on YouTube*, YouTube Help, support.google.com/youtube/thread/313644973/third-party-ai-trainability-on-youtube?hl=en&sjid=17310162182401277271-NC (accessed 10 November 2025).

Ziaja, GM 2024, 'The text and data mining opt-out in Article 4(3) CDSMD: adequate veto right for rightholders or a suffocating blanket for European artificial intelligence innovations?', *Journal of Intellectual Property Law & Practice*, vol. 19, no. 5, pp. 453–459.