Ashurst

Sponsored by Google

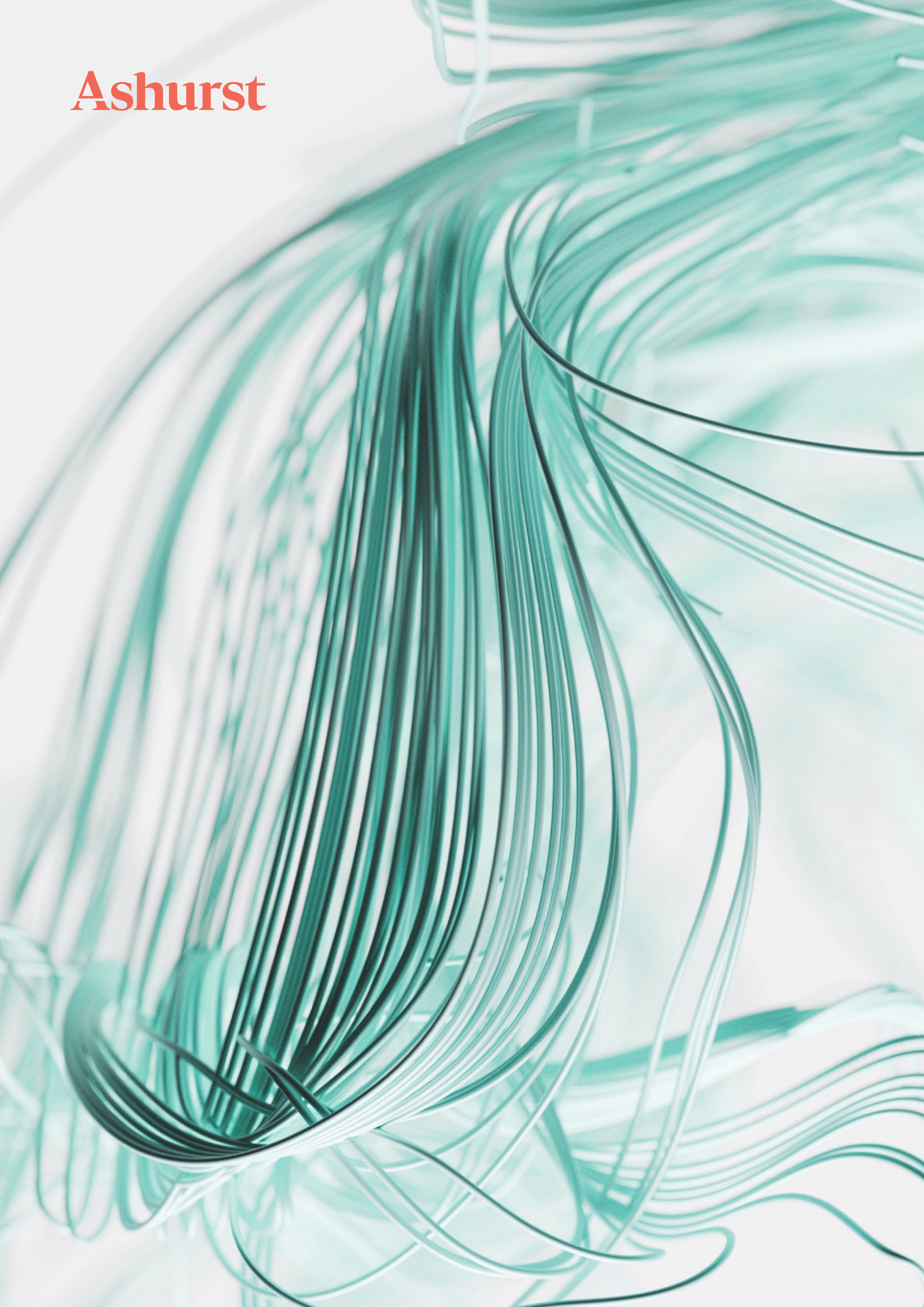
Navigating the Legal Landscape

AI in Australia

A legal deep dive into consumer, privacy, employment, misinformation / disinformation and foreign interference laws

Outpacing change

Ashurst



Navigate this document by clicking on the icons

Navigating the Legal Landscape

AI in Australia

About this paper

Navigating the legal landscape: AI in Australia is an Ashurst paper that has been sponsored by Google.

Our paper assesses how existing legal frameworks in Australia apply, or are likely to apply, to the rapidly evolving field of artificial intelligence (**AI**). It covers the following targeted areas of law:[1]

- consumer law;
- privacy law;
- employment law;
- misinformation / disinformation; and
- foreign interference.

The authors acknowledge the relevance and application of other areas of law to AI, including competition law, copyright law, negligence, the *Corporations Act 2001* (Cth), and sector-specific and profession-specific requirements. They are beyond the scope of this paper.

Australia is grappling with how best to regulate the risks posed by AI, while ensuring we can harness its benefits. Different views have been expressed about the extent to which existing laws already apply to applications of AI, and are fit for purpose. Similar debates are occurring internationally, and no consensus has emerged on the best approach for regulating AI.

The purpose of our paper is to illustrate how Australia's existing laws apply to AI-enabled products and services, offering insights for policymakers, technology companies developing and deploying AI, and businesses using, or considering using, AI in their operations. To that end, we have devised several fictitious case studies (in some cases, inspired by real-life scenarios) involving the use of AI-enabled products and services by consumers and businesses, resulting in a range of potential harms.

We find that the targeted areas of law we considered:

- are technology-agnostic;
- already apply to AI systems, and AI-enabled products and services; and
- appear capable of addressing foreseeable risks from AI systems, and AI-enabled products and services that are commonly used by consumers and businesses, or are likely to be used in the near future.

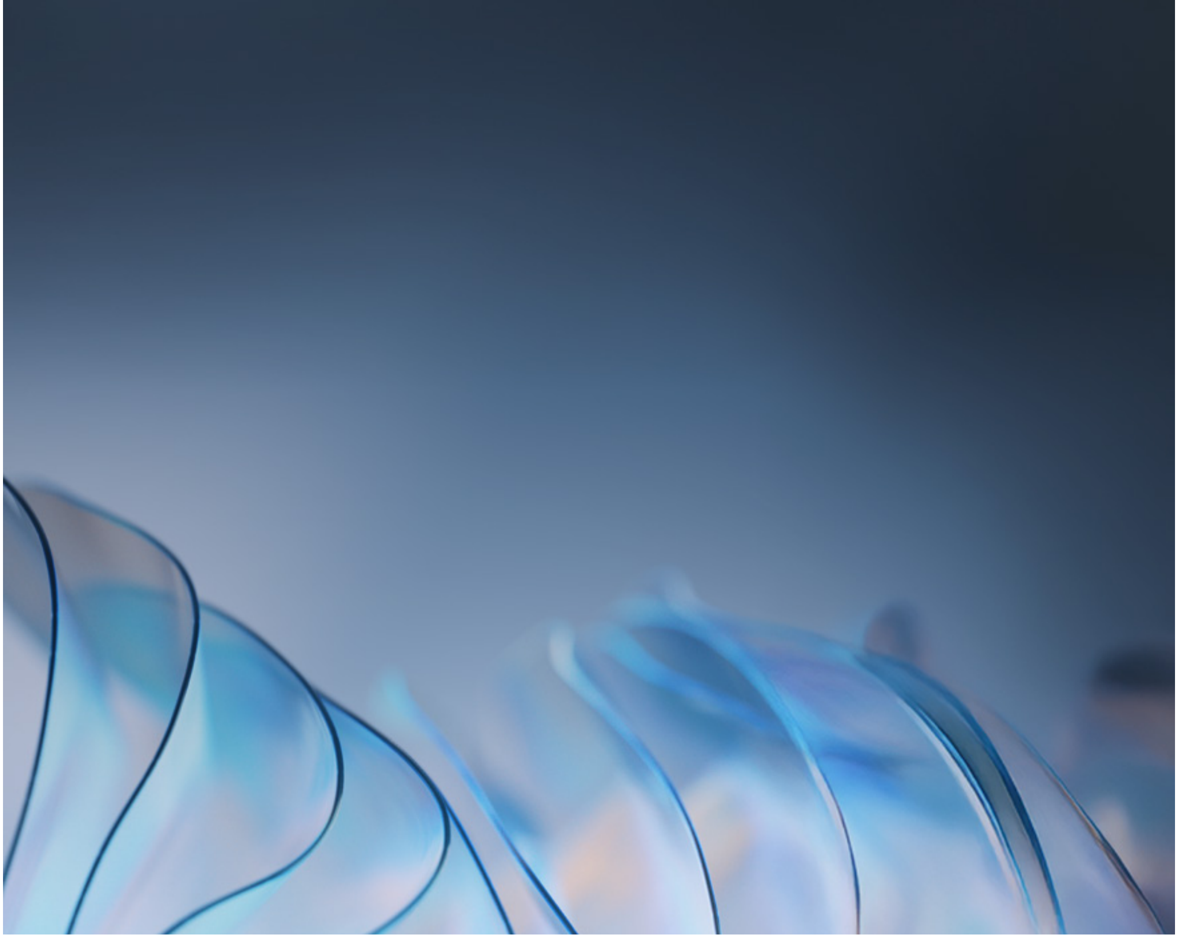
AI can be applied in many different ways, across many industries and used by many different types of businesses and consumers, in high and low risk settings. The risks posed by the use of AI in certain healthcare settings, for example, are, self-evidently, much greater than those posed by the use of AI in entertainment or retail recommender systems, using chatbots to plan holidays or meals, or using an internal enterprise chatbot to help find or file documents, or understand internal policies. Our paper does not seek to cover the field in this regard. Sectors such as healthcare, vehicles, transport and critical infrastructure, where certain uses of AI have the potential for severe consequences (such as death or personal injury) are already heavily regulated, generally in technology-agnostic ways.

Any additional risks posed by AI in those settings might be more appropriately regulated through modifications to existing sector-specific regulation, rather than the introduction of AI- specific legislation that, to a significant extent, duplicates existing laws.

Our case studies and the public materials reviewed in the course of preparing this paper also highlight that Government can usefully play a role in uplifting awareness and initiatives aimed at:

- ensuring businesses (particularly SMEs) deploying AI applications, supplying AI-enabled goods or services, or otherwise using AI in their operations understand their existing legal obligations and have in place robust governance arrangements;[2] and
- ensuring Australian consumers (particularly older Australians who are not 'digital natives') and SMEs are educated about the basics (and inherent limitations) of AI and its appropriate and responsible use.[3]

More effective enforcement of existing laws (including a greater willingness by regulators to run test cases) and more specific guidance from regulators, and/or endorsement of existing or emerging market-based solutions, also have an important role to play.



This paper is up to date as at 30 June 2025.

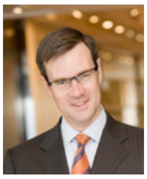
This paper was authored by: Tihana Zuk, Geoff McGrath, Andrew Carter, Trent Sebbens and Robert Todd.

The authors thank (in alphabetical order) Andrew Hilton, Rohan Kumar, Imogen Loxton, Tal Maman, Max Moffat, Kate Pantelidis, Aroon Parthasarathy and Chelsea Toner for their significant contributions.

For transparency, Google was provided with the opportunity to comment on our paper before it was finalised. The paper is our work product, and reflects the views of the authors.

Tihana Zuk
Partner
Competition
tihana.zuk@ashurst.com

Geoff McGrath
Partner
Digital Economy Transactions
geoff.mcgrath@ashurst.com



Andrew Carter
Partner
Dispute Resolution
andrew.carter@ashurst.com

Trent Sebbens
Partner
Employment
trent.sebbens@ashurst.com

Robert Todd
Senior Consultant
Dispute Resolution (IP/Media)
robert.todd@ashurst.com

Introduction

Machine learning and traditional, predictive, AI has been used across many industries since the 2000s. Over the past decade, generative AI has gone from theory to ubiquity — from novel, experimental applications to tools that are now widely used by consumers and businesses, large and small.

It has been observed that '*Defining AI can resemble chasing the horizon: as soon as you get to where it was, it has moved somewhere into the distance.*'[4] In this paper, we adopt the OECD's definition of an AI system as '*a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment*'.[5] An AI system is an application deployed to accomplish a specific function. AI systems are made up of a variety of components, including an AI model.

The OECD's definition is broad enough to capture the traditional, predictive-style AI systems that have long been used, and the more recent, and fast developing, generative AI systems, based on artificial neural networks, that are capable of creating new content including text, code, images, sounds and videos, in response to user prompts. These systems have the potential to transform every aspect of our economies and societies.[6] This can be by enhancing wellbeing and quality of life, for example, by providing personalised healthcare solutions or expediting the discovery and development of new medicines, vaccines or cancer treatments, or by offering intelligent personal assistants that help us manage daily tasks. The systems can revolutionise industries by streamlining production processes, automating tasks and optimising efficiency. They can drive innovation by supercharging research and analytics capability, enabling the development of useful new products, services and business models. They can boost productivity growth and generate new employment opportunities.[7]

While offering immense potential, AI also presents a range of risks. As acknowledged by the Productivity Commission, there are risks that without proper implementation or oversight, AI could be used in ways that harm individuals, businesses, the economy and/or society.[8] This includes harm from errors due to low quality technology or from malicious or reckless use, such as the creation of deepfakes and enhanced cyberattacks. Beyond these, a growing concern stems from the increasing autonomy of AI systems, where significant decisions are being delegated to AI systems, often with insufficient human oversight. These concerns are exacerbated by the 'black box' phenomenon, which arises from AI systems engaging in unsupervised learning, making it difficult — if not impossible — to understand the basis for AI-driven decisions. Other longer term harms that are commonly raised (but are, at this stage, more speculative) include mass job impacts,[9] environmental impact due to increased energy and water consumption by AI data centres,[10] increasing concentration of wealth and power in a few businesses, and widening disparity between high-income and low-income countries.[11]

Globally, the pace of AI adoption is accelerating, with countries making significant investments in AI research and development to maintain or attain competitive advantages.[12]

> 'Defining AI can resemble chasing the horizon: as soon as you get to where it was, it has moved somewhere into the distance.'[4]

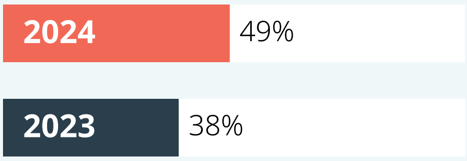
Globally, the pace of AI adoption is accelerating, with countries making significant investments in AI research and development to maintain or attain competitive advantages.[12]

The CSIRO estimated AI will be worth over $22 trillion to the global economy by 2030.[13] Forecasts about the growth impact of AI vary widely, with projections ranging from 1% to 20% of global GDP by 2034.[14] Focusing on Australia, it has been estimated that the adoption of AI and automation could add between $170 to $600 billion to our GDP each year.[15]

While AI is expected to grow our economy, and global investment is increasing,[16] adoption rates of AI across Australia have, until recent times, been relatively low.[17] There is a lack of up-to-date, comprehensive data on the current uptake of AI technology by Australian businesses and consumers.

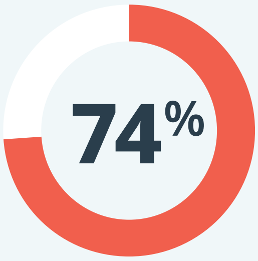
Several statistics and sources suggest adoption is on the rise:

Australians using generative AI



A survey conducted by Google with IPSOS, as part of a global study of 21 countries, reveals **more Australians than ever before are using generative AI** — 49% in 2024, compared to 38% in 2023.[18]

Australian businesses using AI in 2023



Another survey, cited by the Productivity Commission in its 'Making the most of the AI opportunity — Research paper 1: AI uptake, productivity, and the role of government', suggests that **74% of Australian businesses were using AI in 2023**, and 67% of the remainder planned to start using it within the next two years.[19]

About this paper
Introduction
Case studies
Concluding remarks
Annexure

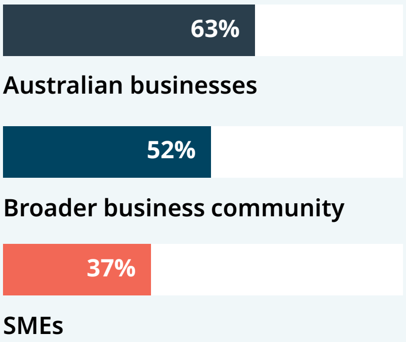
Adoption of AI by Australian financial services licensees

21/23

licensees surveyed reported at least one AI use case that impacted consumers

ASIC's 'Beware the gap: Governance arrangements in the face of AI innovation' report found that adoption of AI by Australian financial services licensees is increasing rapidly. **Of 23 licensees surveyed, all but two reported at least one AI use case that impacted consumers**, with some licensees reporting more than 100 use cases, and 61% reporting they planned to increase their use of AI in the next 12 months.[20]

AI adoption has accelerated significantly across industries



The National Artificial Intelligence Centre observes 'there is a clear consensus that adoption has accelerated significantly across industries over the past 2-3 years', citing studies that estimate **37% of SMEs have adopted AI use**, a **52% rate adoption across the broader business community**, and an estimated **63% of Australian businesses using generative AI tools in 2024**.[21] Further, a survey on AI deployment by the Governance Institute of Australia reported a **90% AU adoption rate among survey respondents.**[22]

Using generative AI tools for purposes beyond entertainment

43%

of those aged 25-54 using it for work or business purposes

79%

of those aged 14-17 using it for school or study purposes

A survey commissioned by the Australian Competition and Consumer Commission (ACCC), referenced in its Digital Platform Services Inquiry Final Report, found that many consumers are using generative AI tools for purposes beyond entertainment, with **43% of surveyed users of generative AI tools aged 25-54 using it for work or business purposes**, and **79% of those aged 14-17 using it for school or study purposes**.[23] The survey also found that the usage of generative AI tools was largely driven by young people — only 31% of consumers aged 65+ and 46% of consumers aged 45-64 had used any generative AI tools, compared to 65% of consumers aged 30-44 and 82% of consumers aged 14-29.[24]

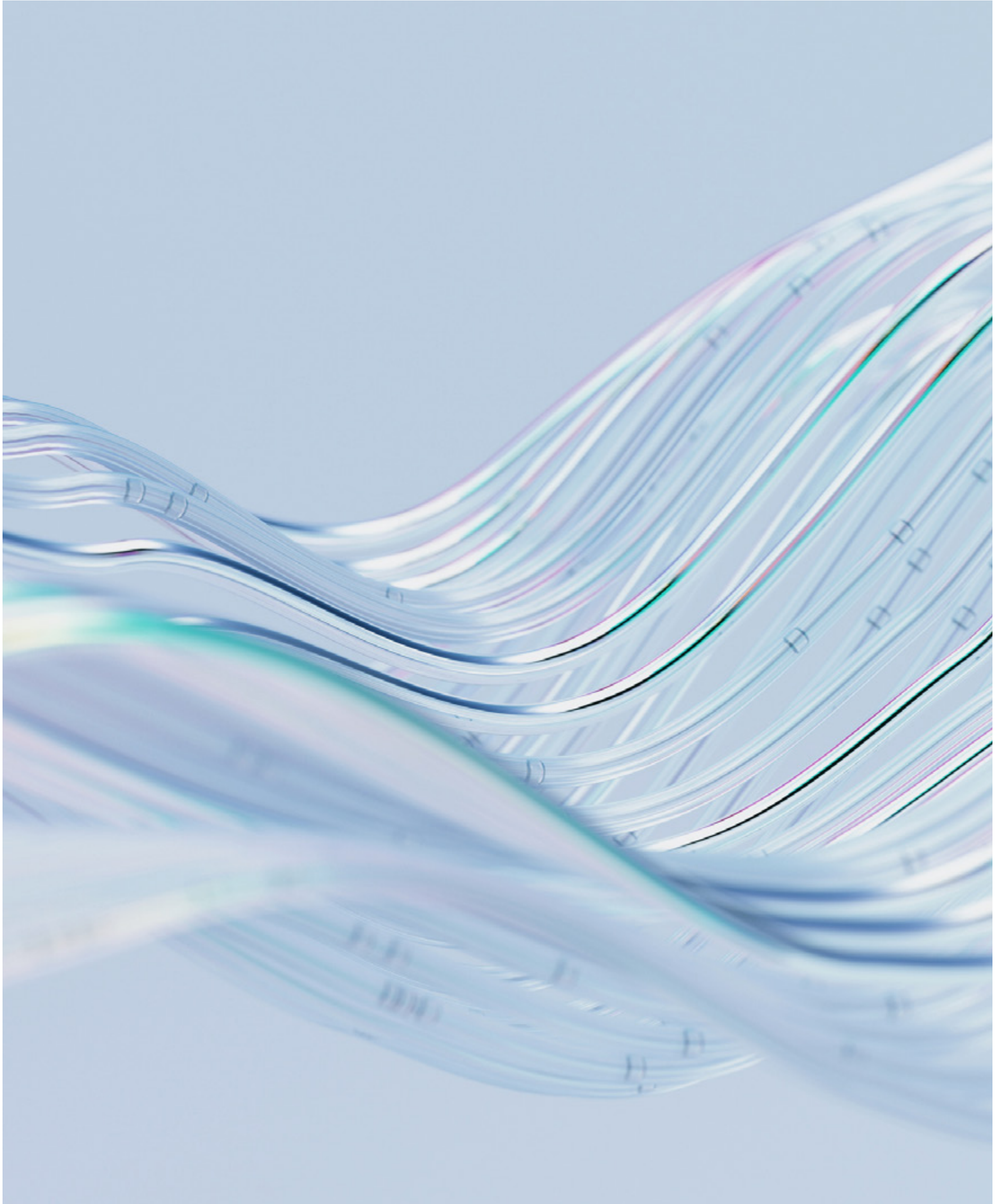
The Productivity Commission has observed that as large software providers embed AI in their applications, **large numbers of their business customers stand to benefit from the functionality of AI** in a relatively frictionless way.[25]

As with the introduction of any new technological advancement, widespread use of AI brings challenges and potential risks.

This includes the risk of consumer harm, privacy violations, cybersecurity risks, the spread of misinformation, and biased decision-making. Many of these types of risks can also arise from the use of other digital, and non-digital, goods and services commonly used by Australians. More advanced AI systems that enable reasoning and agentic behaviour provide unique capabilities, and governments globally are considering whether these unique capabilities, particularly in high risk settings, necessitate new legal frameworks.

This paper aims to provide context to the Australian debate on AI regulation, through an examination of the ways Australia's existing laws relating to consumer protection, privacy, employment, misinformation/disinformation and foreign interference, apply to AI-enabled goods and services.[26] We do so by exploring how our existing laws would apply in the context of several fictitious case studies (in some cases, inspired by real-life scenarios) involving the use of AI-enabled products and services by consumers and businesses.

Next, for context, we give an overview of the state of AI regulation and policy-development globally and in Australia.



Global and local regulatory and policy landscape

Global perspectives on regulating AI

Countries around the world are grappling with whether, and if so, how, to effectively regulate the risks posed by AI. Different approaches have been adopted by early movers, and many jurisdictions are still considering how to strike the right balance between addressing risks and fostering innovation and investment, to harness the benefits of AI. On one end of the spectrum, the European Union has taken a highly prescriptive, risk-centric approach. At the other end, Singapore has taken an approach that addresses what it considers to be the 'real AI governance challenge': how to foster public trust to enable the widespread adoption of AI technologies, including through interventions such as direct subsidies that promote AI uptake in strategic industries.[27]

> Different approaches have been adopted by early movers, and many jurisdictions are still considering how to strike the right balance between addressing risks and fostering innovation and investment, to harness the benefits of AI.

The table below provides a snapshot of key jurisdictions.

Jurisdiction	Key features	Overview
European Union	Mandatory, Prescriptive, Broad / Cross-sector	The European Union Artificial Intelligence Act (**EU AI Act**)[28] became law on 1 August 2024, with enforcement timelines kicking in on a rolling basis starting January 2025. This legal framework was developed over more than half a decade and is the world's first horizontal legal framework for the regulation of AI. The EU AI Act categorises AI systems based on their level of risk ('unacceptable risk', 'high-risk', 'limited-risk', and 'minimal' or 'no-risk'). Notably, the EU AI Act outright prohibits certain AI systems deemed to pose 'unacceptable risk', such as systems which are harmful, deceptive or that exploit vulnerabilities, or which support social scoring systems. Strict obligations are also imposed on so-called 'high-risk' AI systems. Additionally, the EU AI Act also regulates General Purpose AI (**GPAI**) models, and GPAI models meeting thresholds for posing systemic risks. The implementing Codes of Practice are currently being drafted.
United Kingdom	Voluntary, Principles-based, Sector-specific	The UK has adopted a more flexible approach consisting of broad regulatory principles, sector-specific best practices and pre-existing legislation to regulate the use of AI. On 13 January 2025, the UK's prime minister, Sir Keir Starmer, unveiled the UK's AI Opportunities Action Plan, which highlighted the government's pro-innovation approach to AI regulation. The plan includes 50 recommendations aimed at accelerating AI adoption across various sectors, fostering economic growth and enhancing public services, with the ultimate goal of positioning the UK as a global leader in AI.
United States	Sector and Use-case specific, Permissive legal environment	In the US, AI regulation is under debate at the national and state levels. In general, the US-approach focuses on preserving US success in developing state of the art AI technologies, with a strong focus on the geopolitical implications of regulation. Successive presidential administrations and Congresses have chosen not to pursue comprehensive AI-specific federal legislation or regulation akin to the EU AI Act. There are some existing federal laws that address AI systems within certain industries (e.g., aviation, defence),[29] and certain use cases (e.g. autonomous vehicles, the generation of non-consensual intimate imagery). In addition, there are a number of state-led initiatives, for example in California,[30] Utah[31] and Colorado,[32] with the number of enactments rising sharply in the last six years from one bill in 2016 to 131 in 2024.[33] There are also many AI bills being considered by the US Congress, covering a wide range of issues such as AI education, training data disclosure, AI robocalls, biological risks and AI's role in national security. Notably, the House of Representatives passed an initiative to preempt new state laws on AI for a period of 10 years, although the measure is expected to fail on a procedural hurdle. Many of the proposed bills emphasise the development of voluntary guidelines and best practices for AI systems, reflecting a cautious approach to regulation aimed at fostering innovation without imposing strict mandates.

Jurisdiction	Key features	Overview
Singapore	Voluntary, Principles-based, Broad / Cross-sector	Singapore introduced a voluntary Model Framework for AI Governance in 2019 which was subsequently updated in January 2020.[34] The Model Framework is sector and technology-agnostic, and is designed to achieve two high-level guiding principles for the ethical deployment of AI: 1. AI-assisted decision making should be explainable, transparent and fair; and 2. AI systems should be human-centric and safe. The Model Framework translates these ethical principles into implementable practices. In 2024, Singapore introduced the Model Governance Framework for Generative AI. Like the original Framework, it is a living document that is agile, designed to evolve with its adoptees and the fast-paced changes of a digital economy.
Japan	Mandatory, Principles-based, Broad / Cross-sector	On 28 May 2025, Japan passed the Act on the Promotion of Research, Development and Utilisation of Artificial Intelligence-Related Technologies (**AI Promotion Act**). The AI Promotion Act is designed to promote AI R&D, skills, adoption, and the safe use and development of AI to enhance Japan's international competitiveness. The AI Promotion Act empowers the government to require businesses to cooperate in information gathering on the misuse of AI, issue guidance and warn the public when misuse is identified, but it does not stipulate any penalties. The majority of its provisions establish a framework for future laws and policies on AI, rather than imposing specific requirements. Businesses are required to make reasonable efforts to use AI in accordance with the AI Promotion Act's key principles.[35] Japan had previously introduced non-binding AI Guidelines for Business, in April 2024, which were updated in December 2024 and March 2025.

Although the EU AI Act became influential because it was the first and most extensive example of cross-economy AI regulation in the international domain, subsequent economic analysis, for example by former European Central Bank President Mario Draghi, have raised concerns that this approach to regulation is harming the European economy.[36] It now seems less likely to be widely adopted outside of Europe, particularly as the EU itself is reportedly considering pausing or delaying parts of the EU AI Act's implementation due to concerns about its workability and potential stifling of innovation.[37]

The different global approaches to AI regulation and their impacts are a useful reference for the Australian Government as it considers the best way forward for Australia.

The different global approaches to AI regulation and their impacts are a useful reference for the Australian Government as it considers the best way forward for Australia.

About this paper
Introduction
Case studies
Concluding remarks
Annexure

Australia's approach to date

Australia does not currently have AI-specific regulation, but is considering the need to regulate, in particular, in high risk settings. Several consultation processes and reviews are underway on AI regulation, and amendments to existing laws have been proposed.[38]

The Australian Government has made clear that the use of AI is a critical part of future productivity growth in Australia. In December 2024, the Treasurer announced Terms of Reference for the Productivity Commission to undertake five inquiries including into data and technology and AI's productive potential.[39] The Productivity Commission has previously recommended an approach of technology-neutrality and an outcomes-based approach to AI regulation.[40] An interim report (including draft recommendations) is due in August 2025, with the final report due to the Government in December 2025. AI is also likely to be a key feature of the Government's August 2025 roundtable to help inform the Government's growth and productivity agenda.

To date, Australia has responded to potential AI risks through voluntary measures such as the *AI Ethics Principles* published in 2019,[41] and the *Voluntary AI Safety Standard* published in August 2024.[42] The Commonwealth Department of Industry, Science and Resources' consultation into 'Safe and Responsible AI in Australia' indicated that current regulatory frameworks may not sufficiently prevent harms arising from the use of particularly high-risk AI systems.[43] It has published a Proposals Paper consulting on the proposal to introduce mandatory guardrails for AI in high-risk settings. Relevantly:

- The 10 proposed guardrails in the Proposal Paper largely mirror the Voluntary AI Safety Standard, except that the mandatory regime would require conformity assessments (i.e. audit/assurance and public certification), while the voluntary guardrails require broad stakeholder engagement. It is proposed that the mandatory guardrails apply to developers and deployers of AI.[44]

The Australian Government has made clear that the use of AI could be a critical part of future productivity growth in Australia.

A snapshot of the guardrails is below.

1. Accountability	Establish, implement and publish an accountability process including governance, internal capability and a strategy for regulatory compliance.
2. Risk management	Establish and implement a risk management process to identify and mitigate risks.
3. Protect AI systems	Protect AI systems and implement data governance measures to manage data quality and provenance.
4. Testing	Test AI systems to evaluate model performance and monitor the system before deploying it and once deployed, in order to ensure that it remains fit for purpose.
5. Human oversight	Enable human control or intervention in an AI system to achieve meaningful human oversight, which requires organisations to ensure their personnel with oversight understand the AI system, monitor its operation and intervene as needed.
6. User transparency	Inform end users regarding AI-enabled decisions relevant to them, interactions with AI and when end users are being provided with AI-generated content.
7. Contestability	Establish processes for people impacted by AI systems to challenge use of AI or AI-driven outcomes, including by implementing internal complaint handling processes and providing readily available information to impacted parties.
8. Supply chain transparency	Be transparent with other organisations across the AI supply chain about data, models and systems to help them effectively address risks, including by sharing data in relation to adverse incidents and significant model failures, and disclosing risks associated with certain AI systems.
9. Record keeping	Keep and maintain records to allow third parties to assess compliance with the mandatory guardrails, including records relating to the design specifications of the relevant AI system, as well as its capabilities and limitations.

Voluntary guardrails

10 (V). Stakeholder engagement

Engage stakeholders and evaluate their needs and circumstances, with a focus on safety, diversity, inclusion and fairness.

Proposed mandatory guardrails

10 (M). Conformity assessment

Undertake conformity assessments to demonstrate and certify compliance with the mandatory guardrails, which assessments may be performed by the developers themselves, as well as third parties or Government entities/ regulators, both before placing an AI system on the market, and periodically after that to ensure ongoing compliance.

- The Proposal Paper suggested using a principles-based assessment of the intended and foreseeable uses of a system, rather than a list of use cases, for assessing whether AI is 'high-risk'. It also proposed that AI models that are capable of being used for a variety of purposes (or capable of being adapted for a variety of purposes) including by integration would be subject to the 10 mandatory guardrails.
- The Proposal Paper outlined potential options to mandate guardrails, including adapting existing frameworks, creating new framework legislation, amending associated existing legislation or introducing a new AI Act.

Other notable developments include:

- In September 2024, the Government launched its *Policy for the Responsible Use of AI in Government,* setting mandatory requirements for non-corporate Commonwealth entities in the adoption and deployment of AI.[45]
- The Digital Transformation Agency released AI and cyber risk model clauses in March 2025.[46] The clauses aid government buyers procuring services where the seller may be using AI systems in the provision of the services, and bespoke AI systems. The clauses are intended to help mitigate risks and promote transparency and accountability in AI deployment.
- Standards Australia adopted AS ISO/IEC 42001:2003, an international AI management standard that promotes transparency, ethical considerations and comprehensive risk management approaches.

Despite the lack of AI-specific regulation, the supply and use of AI are already subject to a range of existing technology-neutral legislation. This covers consumer protection, privacy, employment, misinformation/disinformation and foreign interference, as discussed in this paper.

Regulators are relying on these existing laws and their existing tools to take action against organisations that have used AI in ways that are alleged to have caused harm.

For example:

- ASIC has brought proceedings against Insurance Australia Limited (IAL) & Insurance Manufacturers of Australia Pty Limited (IMA) for allegedly using an AI-enabled demand model as part of an insurance pricing process that ASIC contends led to the full benefit of advertised loyalty discounts not being appropriately applied.[47]
- The ACCC was successful in proceedings against Trivago in respect of misleading algorithmic decision making.[48]
- The OAIC found that Bunnings breached the Privacy Act by collecting Australians' personal and sensitive information through a facial recognition technology system.[49]

AI-specific risks are also addressed in industry codes and standards under Australia's *Online Safety Act 2021* (Cth). Search engine providers are required to take steps to ensure AI functionality integrated into search engines limits exposure to seriously harmful materials (such as child sexual abuse material) in search results, and to include protections against children being exposed to adult material, including material generated by AI. Generative AI apps and websites need to take steps to limit harmful content such as deepfake intimate content, and to continually improve safety. Similar online safety requirements apply to distributors or marketplaces of AI models. Further industry codes, including for search engines, will apply to age-inappropriate content from 27 December 2025.[50]

Several firms have made public commitments about their development and deployment of AI.[51] For example, Google was one of the first in the industry to publish its AI Principles. It also publishes annual AI responsibility reports detailing its progress.[52] OpenAI has published an AI Charter;[53] Microsoft has identified six principles that should guide AI development and use;[54] Samsung has published AI Ethics Principles,[55] and Salesforce has committed to Trusted AI Principles and guiding principles for responsible agentic AI.[56] IBM has established an AI Ethics Board and committed to a set of guiding principles including fairness, transparency and accountability, as well as establishing a Center of Excellence for Generative AI, which focuses on creating AI that enhances human decision-making rather than replacing it.[57] Developers of advanced AI systems including Google, Anthropic, OpenAI, Microsoft, and Salesforce voluntarily submitted their approaches to risk mitigation as part of the G7 Hiroshima AI Process (HAIP) Transparency Reporting Framework.[58]

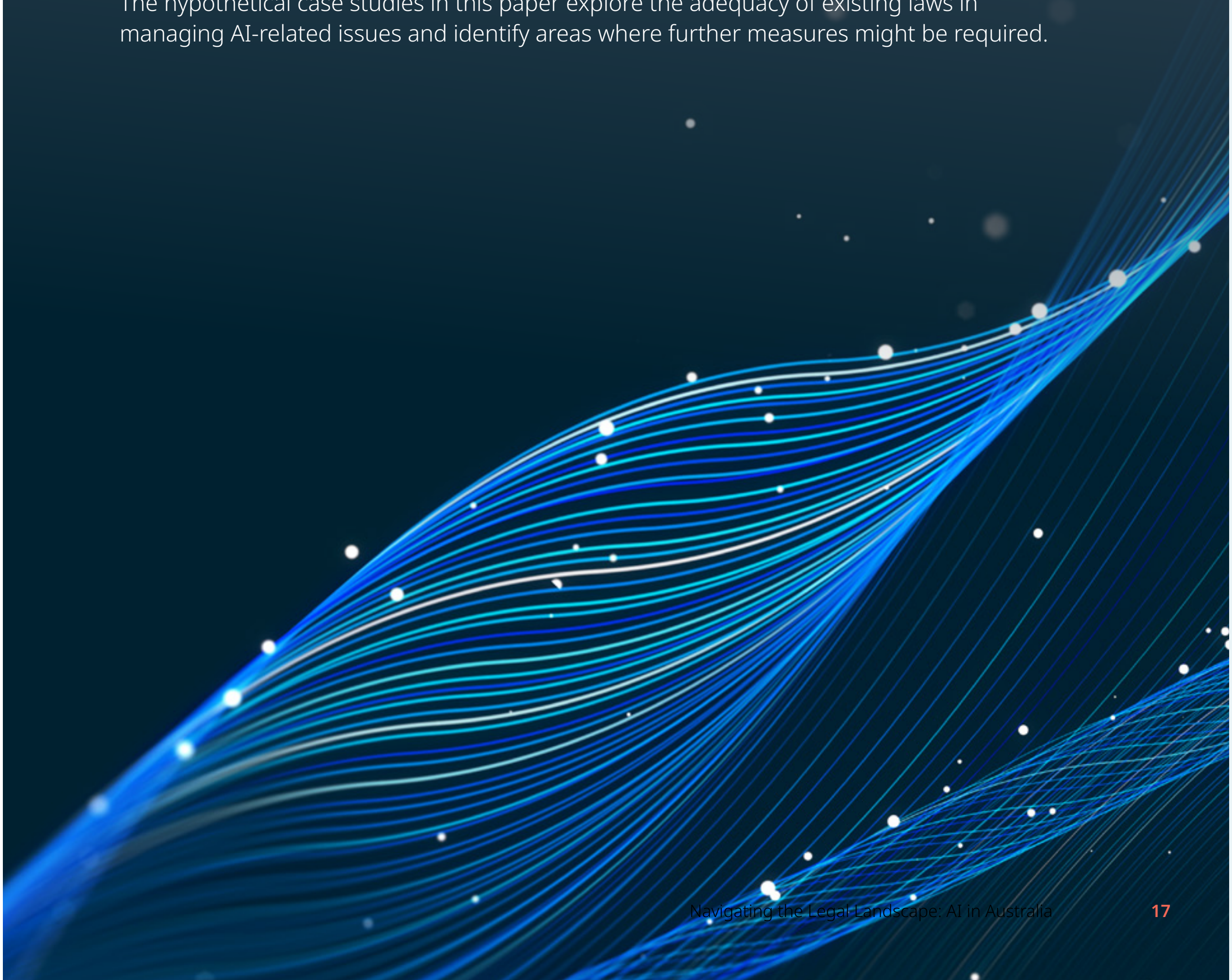
These voluntary measures suggest that social normals and expectations, and market forces, may mitigate some risks without the need for policymaker intervention.

> Regulators are relying on these existing laws and their existing tools to take action against organisations that have used AI in ways that are alleged to have caused harm.

Where to next for Australia?

A starting point for considering any new regulation in Australia is an understanding of the extent to which our existing regulatory frameworks provide safeguards that apply to AI. These existing regulations include consumer, employment, and privacy laws.

The central question is whether existing laws are sufficient to address the risks and challenges posed by AI, or if there are gaps that necessitate new AI-specific regulations. The hypothetical case studies in this paper explore the adequacy of existing laws in managing AI-related issues and identify areas where further measures might be required.



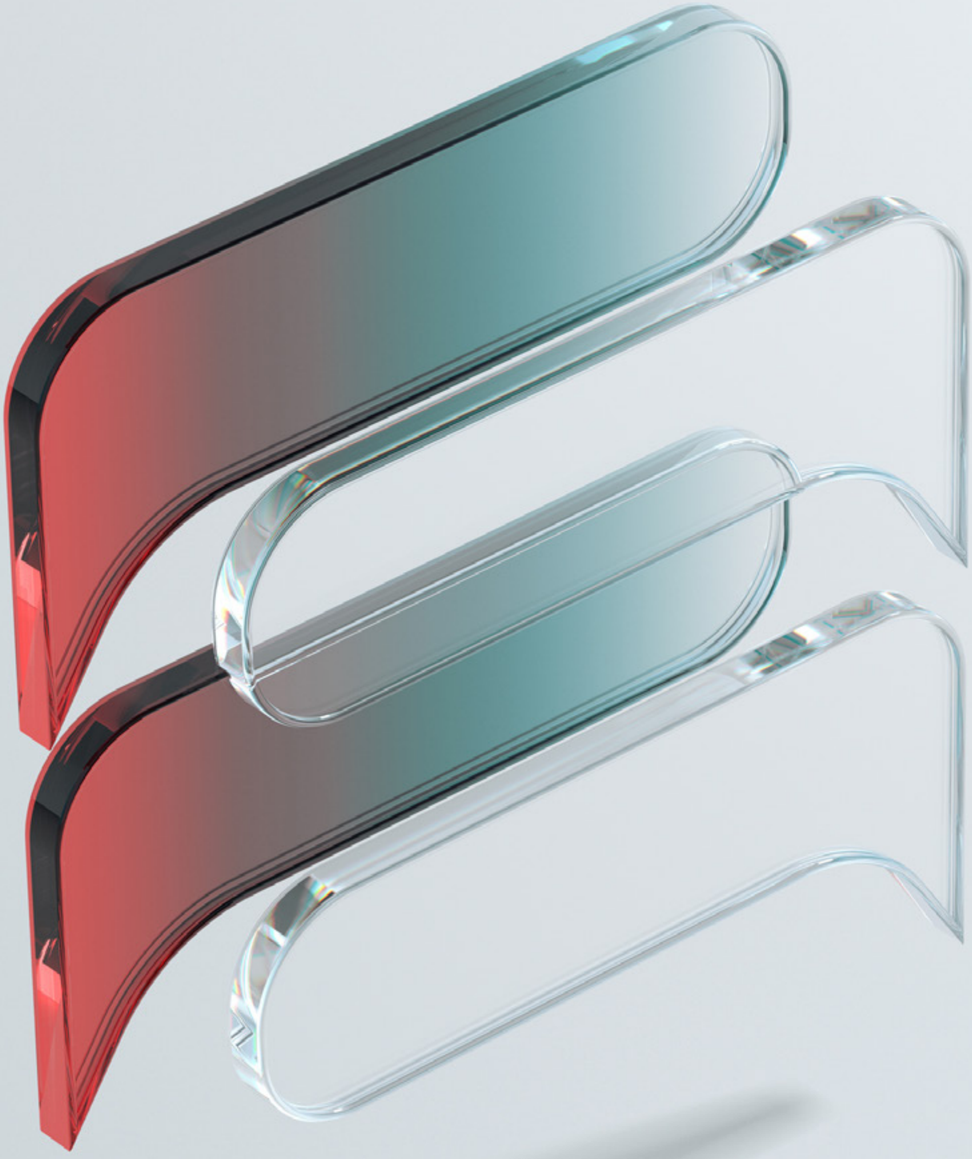
Hypothetical case studies

In this section of the paper we consider eight hypothetical case studies and how existing and proposed laws and regulations in Australia might apply in each case.

- Case study 1: AI chatbots
- Case study 2: AI-enabled smart home device
- Case study 3: AI-powered recruitment tools
- Case study 4: AI in human resourcing
- Case study 5: AI Deepfakes
- Case study 6: AI research assistants
- Case study 7: AI used by foreign states
- Case study 8: AI use by small businesses

Case study 1

AI chatbots



Case study 1

Part A: Consumer law issues

Stratosphere Airlines, a leading global airline offering passenger services in Australia, introduced an AI-powered chatbot named 'StratoAir Helper' accessible from Stratosphere Airlines' website to enhance customer service. StratoAir Helper was designed to assist with flight bookings, provide travel information, and handle customer inquiries.

When a customer accesses StratoAir Helper they are first required to accept standard form Terms and Conditions to use the AI tool. The T&Cs include a broad exclusion of liability clause which exempts StratoAir Helper from all liability including as a result of fault by StratoAir Helper and Stratosphere Airlines. There are no carve-outs or exceptions to this exclusion of liability. There is also no warning that StratoAir Helper may produce outputs that are erroneous.

A customer, Jennie Smith, used StratoAir Helper to book a flight on Stratosphere Airlines for an urgent business trip. The chatbot assured Jennie that she could book a full-fare ticket and later apply for a business travel discount. Trusting this information, Jennie proceeded with the booking. When she later applied for the discount, she was informed by a human representative at Stratosphere Airlines that no such policy existed, leaving Jennie with unexpected expenses.

Additionally, StratoAir Helper used data collected from Jennie's previous interactions and online behaviour to offer personalised pricing. After booking, Jennie noticed that the prices quoted by the chatbot were higher than those available on the airline's website when accessed from a different device.

To make matters worse, Jennie received a follow-up email from what appeared to be Stratosphere Airlines, offering an exclusive upgrade to first class at a discounted rate. The email contained a link to a payment page that looked identical to the airline's official website. Trusting the source, Jennie entered her payment details and funds were deducted from her account, only to later discover that the email was a phishing scam orchestrated by cybercriminals who had exploited vulnerabilities in the AI chatbot's data handling systems.

Part B: Privacy law issues

Using StratoAir Helper, Stratosphere Airlines observed web browsing and application use of users like Jennie, who are looking to book business trips on short notice. Stratosphere Airlines used this information to train the StratoAir Helper AI model to recommend travel arrangements and to optimise pricing decisions (e.g. offering higher prices for short-notice business bookings). Stratosphere Airlines uses StratoAir Helper to generate and fine-tune its assessments and recommendations using a range of public and proprietary data sets, including publicly available training data sets and demographic inferences about individuals (including anonymised information based on behaviours of real users). It does not notify users or obtain their consent to doing so.

As part of the phishing scam described above, the cybercriminals used information about Jennie to personalise the scam, including contact details, travel history, current and future travel plans, travel preferences, and emergency contact information.

Consumer law analysis

The Australian Consumer Law (**ACL**), which sits within Schedule 2 to the *Competition and Consumer Act 2010* (**CCA**), is the principal consumer protection law in Australia. While the ACL does not expressly contemplate AI, there is also no exclusion for AI systems or AI-enabled goods or services. The ACL is technology-neutral and is intended to apply to both traditional and cutting-edge goods and services developed after the ACL's enactment.

The ACL would apply to Stratosphere Airlines to the extent it is carrying on business in Australia.[59] The term 'carrying on a business' is not explicitly defined in the ACL. It is generally given its ordinary meaning and normally involves a series or repetition of acts undertaken for the purpose of profit on a continuous and repetitive basis.[60] Stratosphere Airlines is a global airline, and is involved in the sale of tickets to Australian customers. It engages in marketing activities directed at Australian customers, operates flights between Australia and other countries on a repeated and ongoing basis, and likely incurs expenses in Australia (e.g., airport fees, aircraft maintenance provided in Australia, Australian ground crew salary etc.). For these reasons, Stratosphere Airlines is likely 'carrying on a business in Australia' such that the ACL will apply to its conduct.

Misleading or deceptive conduct / false or misleading representations

The ACL prohibits businesses from engaging in conduct that is misleading or deceptive, or likely to mislead or deceive. This prohibition applies regardless of whether the business intended to mislead or deceive,[61] or whether there is any loss or damage caused as a result of the conduct. Statements, promises, opinions, and predictions can be misleading or deceptive, as can a failure to disclose relevant information.

The prohibitions against engaging in misleading or deceptive conduct and/or making of false or misleading representations can apply to misleading or incorrect information provided to consumers by an AI-enabled good or via an AI-enabled service.[62]

In this scenario, the AI-enabled chatbot, owned and operated by Stratosphere Airlines, misrepresented the availability of a Stratosphere Airlines business travel discount. This misrepresentation was made in trade or commerce and would be attributed to Stratosphere Airlines, as the supplier of StratoAir Helper.

Stratosphere Airlines' use of StratoAir Helper in this scenario might be compared to a business' use of a third-party service provider (e.g. call centre operator) to manage customer complaints, or to provide customer support. Third party service providers in this context are often characterised as 'agents' and misleading representations can be attributed to the business on whose behalf they are operating.[63]

Australian Courts might refer to decisions in overseas jurisdictions (although overseas decisions are not binding on, nor precedential for, Australian courts). For example, in 2024, the British Columbia Civil Resolution Tribunal rejected the argument that an AI-enabled chatbot owned and operated by Air Canada was a 'separate legal entity that is responsible for its own actions', instead noting that 'it should be obvious to Air Canada that it is responsible for all information on its website' and that 'it makes no difference whether the information comes from a static page or a chatbot.'[64]

More generally, the ACCC has made clear that businesses have a responsibility to 'ensure that their algorithms are correct'[65] and should have sufficient checks and balances in place to ensure they do not provide misleading and deceptive information to consumers via AI-enabled goods or services.[66]

If Stratosphere Airlines is found to have breached its consumer law obligations, Jennie may be entitled to recover the loss suffered as a result of relying on the misleading information provided by StratoAir Helper.[67] Stratosphere Airlines may also be liable to significant pecuniary penalties.

Unfair contract terms

The ACL prohibits a business from proposing, using or relying on an unfair contract term in a standard form contract with a consumer or small business.

The broad exclusion of liability clause in Stratosphere Airlines' standard form Terms & Conditions for StratoAir Helper may be considered 'unfair' under the ACL.

This clause purports to have the effect of excluding Stratosphere Airlines' liability for any loss at all, even where Stratosphere Airlines has, for example, breached its own Terms & Conditions or applicable laws, and that breach has caused the user to suffer loss. This creates a significant imbalance between the parties' rights and would likely cause detriment to Jennie (or another customer) if relied upon. Whether or not the term is unfair will therefore likely depend on whether it is reasonably necessary to protect Stratosphere Airlines' legitimate interests.

Stratosphere Airlines might argue that this term is commercially required because it does not control the output of the AI chatbot, and AI chatbots are not always reliable and may inadvertently 'hallucinate' (that is present false information and fabricated references as facts).

It is also offering StratoAir Helper for free. This is unlikely to be accepted by Australian courts, which have already recognised that companies are responsible for the operation of digital goods and services they choose to deploy within their business, including for example, the computer coding underpinning such goods and services. This position is likely to extend to AI-enabled goods and services. This is particularly so in this case where Stratosphere Airlines has deployed StratoAir Helper to assist customers to purchase services from Stratosphere Airlines and given StratoAir Helper does not contain any warning that it may produce erroneous outputs.

If this term is found to be in breach of the unfair contract terms regime in the ACL, the term would be void (i.e., unenforceable), Jennie would be entitled to compensation from Stratosphere Airlines for loss suffered as a result of the breach, and Stratosphere Airlines would be exposed to potentially significant pecuniary penalties.

Consumer guarantees

Stratosphere Airlines must comply with the consumer guarantees under Part 3-2 of the ACL whenever it supplies goods or services to consumers in trade or commerce. In this case, Stratosphere Airlines provided a service to Jennie, being the right or benefit of using StratoAir Helper to answer questions and concerns and to otherwise assist her purchase of an airline ticket.

Although the customer support services in this case were supplied 'free of charge', in that Jennie did not pay any consideration to use StratoAir Helper, these services were still supplied by Stratosphere Airlines in trade or commerce (which can include business activity engaged in for profit, or not) and are of a kind ordinarily acquired for domestic, personal or household use or less than $100,000.[68]

The consumer guarantees relating to the supply of services, including that services be provided with due care and skill, and that they be fit for purpose, will apply.[69]

The obligation to provide services with due care and skill requires service providers to use an acceptable level of skill or technical knowledge when providing the services and to take reasonable steps to avoid loss or damage when supplying the service. When considering whether Stratosphere Airlines provided the service (via StratoAir Helper) to Jennie with due care and skill, it might be necessary to consider, amongst other things, the nature and extent of any training and testing performed on the chatbot, and whether Stratosphere Airlines knew, or ought to have reasonably known that StratoAir Helper might provide inaccurate advice but nonetheless proceeded to launch the service and not warn consumers of this risk.

If it were found that Stratosphere Airlines failed to comply with the consumer guarantees, Jennie would be entitled to seek compensation for any consequential or associated loss or damage resulting from failure, provided the loss or damage was reasonably foreseeable.

Issues with algorithmic personalised pricing

In this scenario, the prices quoted by StratoAir Helper were higher than those available on Stratosphere Airlines' website, which could be a result of the airline engaging in algorithmic price personalisation.[70]

Algorithmic price personalisation is the practice of setting tailored prices for goods or services based on an individual's consumer data and behaviour, aimed to align with their willingness to pay.[71] Research suggests algorithmic price personalisation is already being used by businesses globally, including in Australia.[72]

Commercial conduct designed to influence consumer behaviour and exploit psychological biases – known as 'choice architecture' – can be harmful if it influences consumers to 'purchase unneeded or unsuitable products, spend more than they want to, receive poor-value items or service, choose an inferior seller or platform, or spend less time or effort searching for alternatives'.[73]

Personalised pricing could potentially contravene existing prohibitions in the ACL. For example, pricing which is targeted at exploiting some kind of vulnerability or special disadvantage could be challenged under section 21 of the ACL, which prohibits a business from acting in a way that is, in all the circumstances considered 'unconscionable'. Unconscionable conduct is behaviour that is so harsh, oppressive or unfair, that it goes against good conscience, and beyond what is considered necessary or reasonable in the market.

Algorithmic price personalisation could also fall foul of the prohibition on misleading or deceptive conduct. For example, if it is accompanied by representations that the price is the 'best price', when other consumers are able to access cheaper offers, or representations about discounts or savings accruing to the consumer.[74] Depending on the circumstances, a failure to disclose that pricing is personalised could contravene the prohibition on misleading or deceptive conduct.[75]

The Government is proposing to introduce a prohibition on unfair trading practices, which may also be applicable to this scenario when introduced.[76] The proposed prohibition would capture conduct (regardless of the existence of any vulnerability or disadvantage) where it unreasonably[77] distorts or manipulates, or is likely to unreasonably distort or manipulate, the economic decision-making or behaviour of a consumer and causes, or is likely to cause, material detriment (financial or otherwise).

While the precise scope and application of the proposed prohibition on unfair trading prohibition are yet to be determined, Treasury has acknowledged the possibility of specific prohibitions against dynamic pricing (in this context, pricing that changes during the sales process) and other related pricing practices which may extend to capture personalised pricing.[78]

Scams

The phishing scam is a case of highly opportunistic fraud committed by cybercriminals. In Australia, this kind of conduct is typically dealt with by the Australian Federal Police (including via the Joint Policing Cybercrime Coordination Centre and collaboration with overseas authorities) under the Crimes Act and Criminal Code.[79] There are obvious challenges in identifying the perpetrators of scams that occur online and enforcing provisions of the Crimes Act and Criminal Code against individuals based in jurisdictions that are highly unlikely to have extradition treaties with Australia.

The Australian Government has acknowledged these challenges and recent reforms to the *Competition and Consumer Act 2010* (Cth) are intended to ensure consumers are safeguarded from scams and are able to access compensation when scams do occur.

> The Scams Prevention Framework, which came into force on 21 February 2025, will require regulated entities to take reasonable steps to (amongst other things) prevent, detect and respond to scams.

The obligations will initially apply to regulated entities in the following sectors: banking, telecommunications, and digital platform services, including social media, paid search engine advertising, and direct messaging (upon designation by the Minister). Under the Scams Prevention Framework, once regulated entities are designated and the law takes effect, Jennie could initiate a dispute with her bank (using the bank's internal dispute resolution process, or the external dispute resolution scheme to be administered by Australian Financial Complaints Authority). If Jennie's bank did not comply with the Scams Prevention Framework, or applicable code obligations, Jennie may be able to recover compensation from her bank for loss suffered.

Privacy law analysis

Australia's Privacy Act regulates what organisations can do with personal information, including through limits on collection, use and disclosure, and transparency requirements. These principles are technology-agnostic and apply to AI use cases as they would for other activities.

> AI presents new challenges – and innovative use cases require in-depth analysis and interpretation of laws designed in a pre-AI age – but it is fundamentally not exempt from existing laws.

Notice of StratoAir Helper's AI training activities

Jennie may not be aware that her online activities and behaviours (in particular, unrelated web browsing activities) are influencing StratoAir Helper's process, or *how* the information is influencing the responses provided by StratoAir Helper.

Stratosphere Airlines' use of Jennie's interaction with the StratoAir Helper app to train StratoAir Helper may be authorised under the Privacy Act (as a reasonably expected secondary purpose related to the primary purpose). The Privacy Act requires Stratosphere Airlines to take reasonable steps to ensure Jennie is aware of the *purposes* for which personal information is to be used or disclosed. Transparency will improve the likelihood that Jennie may reasonably expect those AI uses. In some cases a broader statement may be sufficient, but in others more specific disclosures may be needed (particularly where the AI use may not be apparent).

Security of personal information

In the phishing scenario, the cybercriminal has deliberately manipulated StratoAir Helper so it is able to have unauthorised access to detailed information including about Jennie's previous travel arrangements and travel preferences. This could be used by cybercriminals to send Jennie phishing emails or texts (like the one she received), and also sold on to other cybercriminals. Although this type of manipulation is specific to AI models, it relates to the security of personal information generally.

The mere fact that StratoAir Helper was manipulated so a cybercriminal could access Jennie's data does not, by itself, mean that Stratosphere Airlines has breached its privacy obligations. Stratosphere Airlines is required to take reasonable steps to protect personal information, including by implementing technical and organisational measures. The 'reasonable steps' required will depend on a number of factors, including the nature of the entity, the personal information to be protected, as well as practical implications such as time and cost of implementing security measures.

What is considered a reasonable step will evolve over time and will require a degree of ongoing monitoring and continuous improvement.

Because cybercriminals had access to and extracted Jennie's travel information, Stratosphere Airlines will be required to investigate whether a data breach is notifiable (i.e. if it is likely to give rise to 'serious harm' to Jennie) and, if so, report it to the privacy regulator, Jennie and potentially other customers.

Case study 2

AI-enabled smart home device

Case study 2

Part A
Consumer law issues

CuttingEdge Innovations, a leading manufacturer and supplier of smart home devices, started selling a new AI-powered smart refrigerator called 'SmartFridge Pro'. The company marketed SmartFridge Pro as a revolutionary appliance equipped with advanced AI algorithms capable of managing grocery inventories, automatically ordering food, and optimising energy consumption. The marketing materials emphasised the refrigerator's ability to learn user preferences, prevent food spoilage, and reduce energy bills.

One customer, Mick Brown, experienced significant issues when the refrigerator's AI system malfunctioned. The AI system failed to recognise the correct inventory levels and repeatedly ordered excessive amounts of groceries, resulting in a huge grocery bill. Additionally, the AI system periodically adjusted the refrigerator's temperature settings to freezing, causing food to freeze and defrost repeatedly (resulting in higher energy bills), and in some cases spoil or lose taste and quality.

Investigations revealed that the AI algorithms used in SmartFridge Pro were not as advanced as advertised and that the device often relied on outdated data and simplistic decision-making processes. CuttingEdge Innovations had exaggerated the AI capabilities of SmartFridge Pro in its marketing materials, leading consumers to believe that the appliance was more sophisticated and reliable than it actually was.

When Mick sought a refund or replacement for his defective refrigerator, CuttingEdge Innovations argued that the problem was due to user error and/or external factors, rather than a defect in the AI system. It alleged that the malfunction was caused by changes to the AI system that occurred after Mick had purchased the refrigerator. Mick frequently adjusted the temperature settings manually, and the AI system adapted to these changes, which compromised its ability to maintain optimal temperature settings. CuttingEdge Innovations refused to provide Mick with a refund or replacement.

Part B
Privacy law issues

Mick and his 12 year old child Fuzail suffer from obesity and are attempting to cut down their food consumption levels. The SmartFridgePro refrigerator infers from Mick's recent grocery inventory choices, proprietary data sets and data collected by the refrigerator, that Fuzail is at high risk of diabetes and heart disease. Some of this data is collected from a hidden, high-definition camera installed in the refrigerator that records each instance Mick and Fuzail visit the refrigerator, and a video and audio stream of their conversations in the kitchen. CuttingEdge Innovations does not disclose this video and audio recording function in its materials about the SmartFridgePro.

Using this data, CuttingEdge Innovations creates a comprehensive profile that includes Fuzail's contact information, characteristics and health risks in a large targeted marketing database that has been specifically created to sell to a marketing agency to advertise invasive and high-risk experimental weight loss surgeries to young people. The marketing agency inputs Fuzail's profile to an AI model that has been specifically trained to heighten feelings of insecurity in young people, generating hyper-personalised ads that focus on Fuzail's food choices and emotional triggers.

Buried in SmartFridgePro's terms of use is a notice that CuttingEdge Innovations uses personal information for various vague and broad purposes, including to provide 'personalised information and services' without any more detail.

Consumer law analysis

Misleading or deceptive conduct / false or misleading representations

There is growing demand for goods and services powered by AI, with consumers becoming more willing to pay a premium for AI-enabled goods and services.[80]

Given this trend, it is likely that the ACCC will closely scrutinise claims made by businesses regarding their use of AI in the supply of consumer goods or services to ensure they are not false or misleading (an act which has been termed 'AI-washing').

The ACCC has already demonstrated its commitment to protecting consumers from deceptive practices, including in respect of 'greenwashing' – the act of making false or misleading claims about the environmental benefits of products or services. Greenwashing is one of the ACCC's key enforcement priorities for largely the same reasons (i.e., because consumers are willing to pay a premium for sustainable or environmentally friendly goods and services). The rising prominence of AI claims in the market is expected to trigger similar levels of vigilance from the ACCC to ensure that businesses provide accurate and transparent information to consumers.

There have been several recent AI-washing cases in other jurisdictions,[81] including in the United States where two investment advisers, Delphia Inc and Global Predictions Inc, were required to pay US$400,000 (~$600,000) in penalties for false and misleading marketing, which breached US securities rules and regulations. The companies claimed that their investing algorithm used AI and machine learning in its process including, for example, to 'predict which companies and trends are about to make it big and invest in them before everyone else', which was not true.

The ACL prohibitions regarding misleading or deceptive conduct and false or misleading representations are technology-neutral, and would clearly apply to representations regarding AI-enabled goods or services. In this case, the representations made by CuttingEdge Innovations in its marketing were false or misleading. The SmartFridge Pro did not have advanced AI capabilities and could not function as advertised. Accordingly, CuttingEdge Innovations is likely to be in breach of the prohibitions on engaging in misleading and deceptive conduct and/or making false or misleading representations, and could be liable to pay damages and be exposed to potentially significant pecuniary penalties.

Consumer guarantees

The consumer guarantees under Part 3–2 of the ACL would apply to this transaction because the goods or services being supplied by CuttingEdge Innovations are 'consumer' goods or services – in other words, they are of a kind ordinarily acquired for personal, domestic or household use or were likely acquired for less than $100,000.

AI-enabled goods and services, such as smart locks, network connected refrigerators, wearable health trackers and smart home assistants, are complex and usually consist of hardware, software and associated services.[82]

The ACL's definitions of 'goods' and 'services' are broad and inclusive, and the distinction between the two is important because it determines which of the consumer guarantees apply to the transaction and the types of remedies available to the consumer in the event of a breach.

In transactions involving both the supply of goods and services (ie, mixed supply) a consumer cannot claim a remedy for both a faulty good and a faulty service.

It is likely that in this case, the supply of the SmartFridge Pro to Mick will be characterised (at least) as a supply of consumer 'goods'. This is because the definition of 'goods' under the ACL includes certain digital products, for example computer software.[83] In a 2018 case involving Apple, it was confirmed that the definition of 'goods' also extends to software updates, which occur after the supply of a product or service.[84]

CuttingEdge Innovations must comply with the guarantees relating to consumer goods. On the facts, it is likely that the SmartFridge Pro would not meet several consumer guarantees, including:

- the guarantee of **acceptable quality**, as the device is not fit for all (or any) of the purposes for which a reasonable consumer would typically acquire a smart fridge, and appears to be defective and unsafe (particularly as it has reportedly caused food to spoil).
- the guarantee as to **fitness for purpose**, as the device is not fit for the specific purposes advertised by CuttingEdge (ie, 'managing grocery inventories, automatically ordering food, and optimising energy consumption').
- the guarantee as to **supply by description**, as the device does not meet the description in marketing materials, which portray the device as being a 'revolutionary appliance equipped with advanced AI algorithms'.

The failure to comply would be a 'major' failure, if an ordinary, reasonable consumer would not have purchased the device had they known there were defects with the AI system, which would significantly impact the fridge's functionality and ability to perform as intended. In the case of a major failure, a supplier is required to remedy the consumer by providing a refund or replacement of the product or providing compensation for any decrease in the value of the product as a result of the failure(s). It is also required to compensate the customer for any reasonably foreseeable loss occurring as a result of the failure.

Here, CuttingEdge Innovations has refused to provide Mick with a refund or replacement on the basis that he caused the device to malfunction. Consumers are not entitled to a remedy under the consumer guarantees where the failure was caused by the consumer's misuse of the product. Whether or not Mick misused the SmartFridge pro will depend on a number of factors, including for example, whether a user manual was provided to him with the device, which explicitly warned customers **not** to make manual adjustments to the temperature or other features as it may impact the performance or functionality of the fridge.

The onus is on Mick to prove a breach of the consumer guarantees. Mick would need to demonstrate that he did not act contrary to any clear instructions or warnings (or otherwise, that he was not provided with any such instructions) and provide evidence of his use of the product and that such use did not amount to misuse.

Unless it is established that Mick has misused SmartFridge Pro, CuttingEdge Innovations will be required to remedy the failure. If CuttingEdge Innovations were only the supplier, but not the manufacturer, it may have a right to seek indemnification from the manufacturer of the SmartFridge Pro device, in which case the manufacturer would be liable to reimburse CuttingEdge Innovations for the cost of providing Mick a remedy and any compensation it had to pay for reasonably foreseeable loss.[85]

Product safety

Businesses must comply with product safety obligations under the ACL.[86] In this case, there is a risk that the SmartFridge Pro could cause serious injury (for instance if a consumer were to be hospitalised and treated for consuming spoiled food) which could entitle the individual to remedies under the consumer guarantees regime. It would be prudent for CuttingEdge to consider whether the potential issue could be fixed through an automatically deployed software update, or otherwise whether a voluntary recall of the product is warranted.

Privacy law analysis

Collecting sensitive information

SmartFridgePro's inference about diabetes and heart disease risk is a collection of health information that may breach Australia's Privacy Act if consent is not obtained. Generally, CuttingEdge Innovations is required to obtain consent for the collection of sensitive information, which includes health information. The vague notice buried in SmartFridgePro's terms of use is unlikely to be sufficient.

While there is no fixed age at which a child may give their own consent under the Privacy Act, guidance from the privacy regulator recommends that parent or guardian consent is sought for individuals 15 and under, and it is unlikely a 12 year old would be considered mature enough to provide consent themselves, particularly in the context of the collection or use of sensitive information for advertising an invasive and experimental surgery. Additional protections for children will be included in a new Children's Online Privacy Code, which will be in place by 10 December 2026.

Use of the SmartFridgePro to infer health risks for advertising purposes (particularly in relation to children) without sufficient notice or any consent would likely be considered unreasonably intrusive, resulting in a breach of CuttingEdge Innovations' obligation to collect personal information by 'lawful and fair means'.

Direct marketing and targeting based on sensitive information

The Privacy Act prohibits the use or disclosure of sensitive information for direct marketing unless an individual has provided consent. This will include sensitive information inferred or generated by AI. The vague notice included in SmartFridgePro's terms of use is unlikely to be sufficient.

Proposed changes to the Privacy Act are expected to include a prohibition on targeting individuals based on sensitive information, as well as changes to address specific risks arising from targeting of children, and a new overriding obligation for information handling to be fair and reasonable.

These changes do not form part of the current framework under the Privacy Act.

Additional laws, regulations and industry codes relevant to advertising (particularly relating to health services and children), 'spam' electronic messages, and consumer protection may also apply to the advertising campaign.

Serious invasion of privacy

Fuzail and other young people targeted in the advertising campaign could potentially make a claim against CuttingEdge Innovations for a 'serious invasion of privacy' under recent reforms to the Privacy Act. Some key elements Fuzail would need to prove are that CuttingEdge Innovations misused information or intruded on Fuzail's seclusion either recklessly or intentionally, in circumstances where there was a reasonable expectation of privacy and where the invasion was serious.

In this instance, Fuzail would have a good claim that these elements have been made out, particularly as an intrusion into seclusion given the intentional use of hidden cameras to record audio and video of Fuzail in his home, or a misuse of information by sale of the information to third parties. The level of deliberate intention, lack of transparency, emotional manipulation, specific targeting of young and vulnerable people at scale, coupled with the reasonably likely offence, distress and other potential harms to Fuzail (including the potential for psychological harm from surveillance and subsequent misuse of information), and the likelihood that CuttingEdge Innovations knew or should have known of the risks, would all combine to support Fuzail's claim. Consent is a defence to the new cause of action. Seeking clear consent (from Mick, including as Fuzail's parent) would have given Mick and Fuzail the ability to make an informed choice about CuttingEdge Innovations' activities, and would permit CuttingEdge Innovations to undertake these activities if consent were given.

Case study 3

AI-powered recruitment tools

Case study 3

Shortest Cuts, a large hair care retail chain, decided to use an AI-powered recruitment tool to save time when undertaking a process to hire a new Marketing Manager for one of its locations. The tool was advertised as being capable of reviewing resumes and cover letters to identify a shortlist of candidates for a role and then assessing video interviews to make final hiring decisions.

When setting up the AI software, the company uploaded the resumes of all its current employees and their position titles so that the tool could 'learn' about the composition of the workforce and seek to hire a candidate who would be a good fit in the team. The company's workforce was comprised mostly of men in their 30s; particularly in managerial roles where 90% of employees were male.

The company received 100 applications for the vacant role and solely relied on the AI tool to create a shortlist of 10 candidates without requiring a human resources staff member to review any applications. Nine of these candidates were men as the AI tool had 'learned' that this was preferable for managerial positions.

Each candidate was then asked to record video responses to a series of questions which were again assessed by the AI tool without human oversight to create a ranked list of candidates. The candidates were ranked 1 to 10 in rough order of age from youngest to oldest, with the exception being the female candidate who was ranked 9th and the youngest male candidate who was ranked 10th. This candidate had previously experienced a stroke and suffered partial facial paralysis as a consequence. The AI tool was capable of assessing a candidate's facial expressions during their recorded video responses.

The AI tool did not provide any written reasoning for the rankings. The human resources team offered the position to the top ranked candidate.

Privacy law analysis

Disclosure of resumes to train AI models

Although the 'employee records' exemption under the Privacy Act would usually apply to Shortest Cuts' use of its employees' resumes, there is a good chance that it would not apply in this case on the basis that training an AI tool for recruitment purposes is not 'directly related' to the employment relationship between the relevant employees and Shortest Cuts.

This means normal privacy rules are likely to apply. Shortest Cuts would need to look at the purpose of collection, whether the use is a reasonably expected and related secondary purpose, whether individual employees have given their consent, or whether another exception applies.

Shortest Cuts would need to review its employment agreements and any notices given to employees about how it collects and uses resumes. Another option may be to anonymise the resumes, but simply removing names will not be enough: to be effective, any de-identification would need to be undertaken in such a way that the individual is no longer reasonably identifiable.

Shortest Cuts will also need to be transparent about how it is using candidate information for automated decisions.

New privacy laws due to commence 10 December 2026 will require greater transparency about automated decision-making (including computer assisted decisions) that have a significant impact on the rights or interests of an individual.

Shortest Cuts will need to disclose its use of the recruitment tool, and that applicants' personal information will be used in this process.

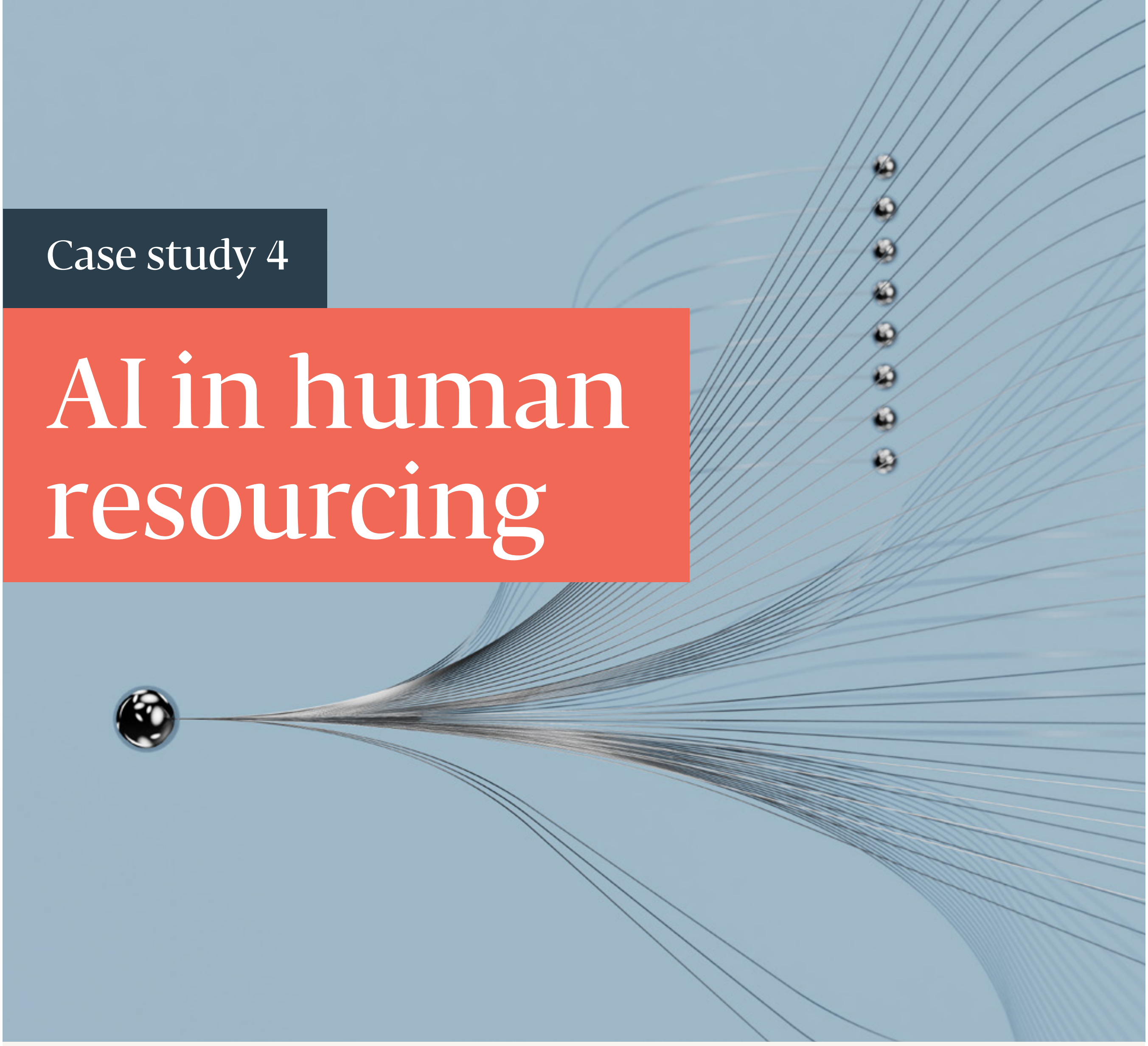
Employment law analysis

In this scenario, Shortest Cuts engaged via the AI tool in direct discrimination by reflecting the latent bias in the existing workforce profile in selecting candidates for the vacant position. It also engaged in discrimination by treating the candidate who had suffered a stroke less favourably than other candidates on the basis of the ongoing disability experienced by that candidate.

This may be a breach of both the general protections provisions in the *Fair Work Act 2009* (Cth) (**Fair Work Act**) and anti-discrimination regimes under Federal and State legislation. While these legislative schemes are unique, they generally prevent discrimination on the basis of a variety of protected characteristics such as age and disability. Their protections are extended to prospective employees as well as current employees.

Under the Fair Work Act, Shortest Cuts would have difficulty in defending a claim in these circumstances as it would bear the onus of proof to demonstrate that it did not refuse to employ particular candidates on the basis of their gender or disability. As the AI tool did not produce reasons for its assessment, Shortest Cuts would be unable to determine whether there was a legitimate basis to the AI tool's ranking of candidates primarily in age order and providing less favourable treatment to the candidate with a disability.

This is similar to real life examples where companies have utilised recruitment tools that have been reported as demonstrating a preference towards male candidates.[87]



Case study 4

AI in human resourcing

Case study 4

Even Faster Fashion, an online clothes retailer, employed casual workers at its warehouse to pack clothes ordered by online shoppers. The company used AI software to monitor how many orders were completed by employees every shift and their attendance at work. The software would reduce an employee's 'productivity' score if they dropped below a certain number of orders per shift, and would also reduce their 'reliability' score if they were late to work or left a shift early. If either of these scores dropped below a particular threshold, the company would prioritise other employees when offering shifts for the upcoming fortnight.

Sarah Brown had been a casual employee at the company for two years and had consistently met the required threshold for the productivity score during that time. Sarah sustained an injury to her back following a serious car accident which meant she had a physical disability and found it difficult to stand for long periods of time. Sarah found that she could still work productively for an hour at a time but then had to take a five minute break to sit down. Sarah's productivity score dropped over the course of a few weeks, and she told her supervisor that she was struggling to keep up due to her disability. Sarah's supervisor did not have control over the roster and the company began to offer Sarah fewer shifts than usual.

Aryan Singh had been a casual employee at the company for one year and had always maintained a high reliability score. Aryan's three year old daughter had recently begun attending daycare and was regularly getting sick as illnesses were passed between children. As a result, Aryan had been late to work and had left shifts early on a number of occasions to pick his daughter up from daycare as he had been unable to make alternative arrangements for her care. Aryan always promptly informed his supervisor when he was running late or leaving early for this reason and would make up for lost time by staying later or starting his next shift earlier, but his reliability score reduced accordingly and the company began to offer him fewer shifts than usual.

Privacy law analysis

Collecting sensitive information about employees

While employee records are exempt from the Privacy Act in many instances, case law has clarified that the Privacy Act will still apply to the process of collecting that information. This may mean, for example, that collecting biometric information (such as face-prints used for facial recognition technology or fingerprints for sign-on processes) as part of Even Faster Fashion's AI tool may require consent unless an exception applies.

Proposed future reforms to the Privacy Act include additional privacy protections for employee records, and the January 2025 Australian Parliament 'The Future of Work' report recommended wide ranging reforms to enhance employee protections in relation to uses of AI like the productivity score system.[88]

New privacy laws due to commence 10 December 2026 will require more specific information to be made available about automated decision-making (including computer assisted decisions) that have an effect on the rights or interests of an individual. Even Faster Fashion will need to be transparent about how it is using employee and contractor information for automated decisions, including the use of the 'productivity' and 'reliability' scores. Due to the employee records exemption, this requirement will not apply to activities and data that is directly related to the employment relationship.

Surveillance of employees

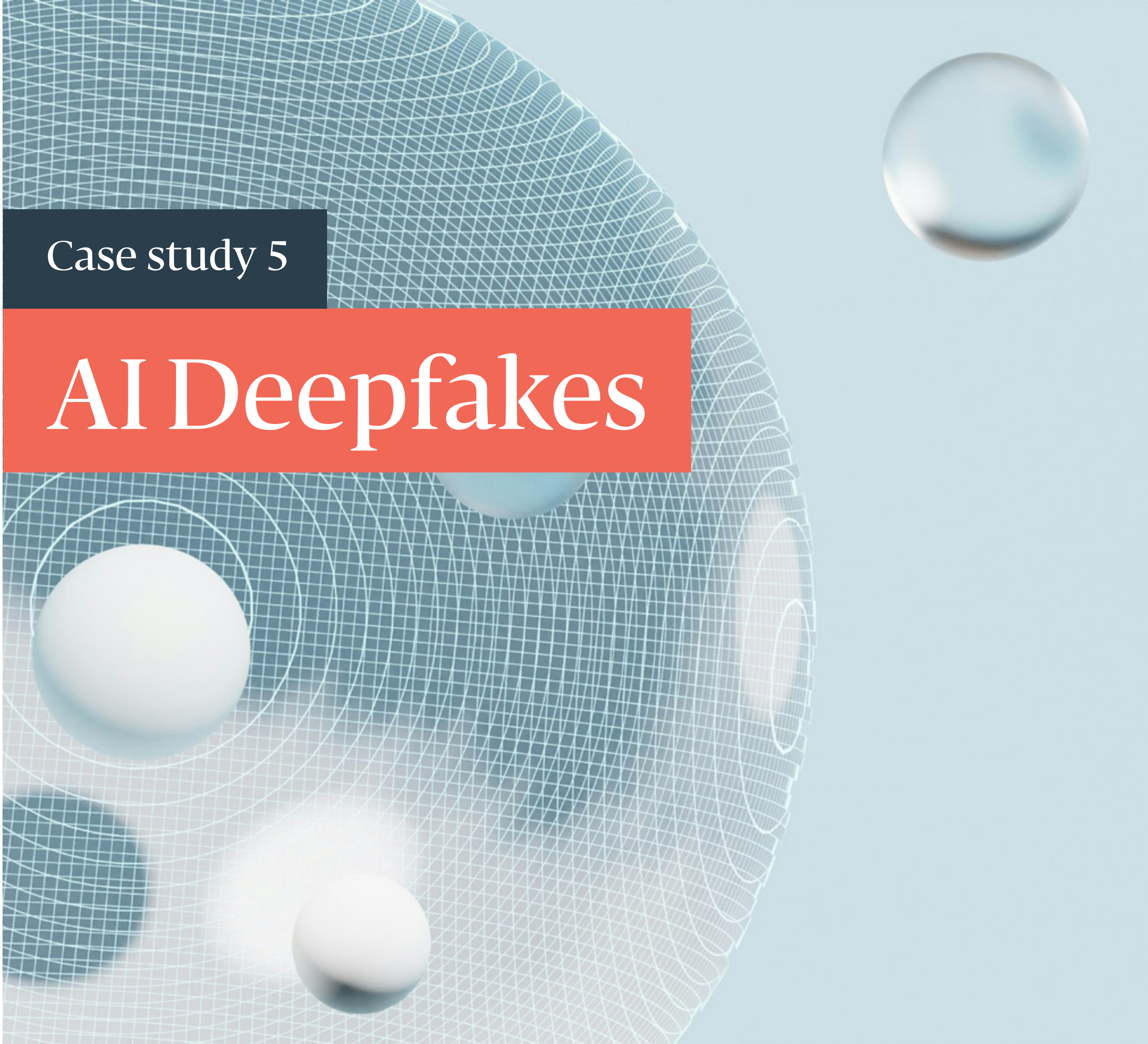
Additional restrictions apply under state-based legislation to workplace monitoring. For example, in NSW and the ACT, Even Faster Fashion would be required to give its employees at least 14 days' prior notice before commencing surveillance. In the ACT, Even Faster Fashion would need to take reasonable steps to protect any surveillance records from misuse, unauthorised access or loss and would need to destroy or de-identify any surveillance records that are no longer needed.

Changes to surveillance laws have been proposed both in the January 2025 Australian Parliament 'The Future of Work' report,[89] and the May 2025 Victorian Parliament 'Inquiry into Workplace Surveillance' report.[90]

Employment law analysis

The AI tool engaged in indirect discrimination by applying the same performance standard to all employees regardless of their personal circumstances which may be protected at law (in this instance, physical disability and caring responsibilities). Like in Case study #3, this may be a breach of both the general protections provisions in the *Fair Work Act* and anti-discrimination regimes which prevent unfavourable treatment on the basis of a person's disability and carer's obligations.

This is similar to a real life example where an AI tool used by a food delivery service offered riders less work if they had cancelled shifts, regardless of their reason for cancelling it.[91]



Case study 5

AI Deepfakes

Case study 5

World-renowned tennis star Carlos Williams finds himself at the centre of a controversy when a video of him goes viral online. The video depicts Carlos confidently endorsing a new line of tennis rackets from a manufacturer, Triumph Sports Gear, despite his long-standing exclusive sponsorship deal with AuraPeak Athletics, a competitor in the tennis racket industry.

The video appears to have been filmed during one of his official post-match press conferences, where he praises the new racket for its 'superior grip' and 'unmatched power.' The video quickly spreads across social media, sparking heated discussions among tennis fans.

As the video gains viral traction, Triumph Sports Gear starts to receive a surge in inquiries about the racket Carlos allegedly uses. Within days, Triumph Sports Gear runs an ad campaign with excerpts from the video, suggesting that Carlos is now part of their athlete roster.

Unknown to Carlos, his management team is alerted to the video when a fan reaches out to express their excitement about Triumph Sports Gear's advertisement and Carlos' supposed new endorsement deal. Initially confused, his team quickly investigates and realises that the video is a sophisticated fake. The deepfake was produced using AI-driven technology that flawlessly mimics Carlos' voice, expressions, and movements, convincing even seasoned tennis fans. His team scrambles to issue a statement, declaring that Carlos has never endorsed or used the Triumph Sports Gear racket and reaffirming his ongoing partnership with AuraPeak Athletics. However, the damage is already done — public perception has shifted, and questions linger about the authenticity of his endorsements.

Even more alarming, sexually explicit deepfake videos start appearing online, conspicuously displaying Carlos with AuraPeak Athletics branded merchandise.

Online safety laws and misinformation

The eSafety Commissioner can direct the removal of certain online content. These takedown powers are limited to certain types of materials, which include altered intimate images shared without consent.[92]

While the initial deepfake videos showing Carlos' endorsement of a competitor's tennis rackets may not meet the threshold for a removal direction, Carlos would likely be able to ask that the eSafety Commission direct the removal of the later sexually explicit deepfake videos.

In addition, Carlos may be able to raise a complaint to platforms hosting the deepfake videos under the processes they are required to maintain under the Basic Online Safety Expectations (BOSE) or have committed to implement under the *Australian Code of Practice on Disinformation and Misinformation*. Under the *Code of Practice*, digital platforms also commit to put in place measures to reduce the propagation of, or user exposure to, misinformation or disinformation, which may include removal of certain content. Users are also able to report content or behaviours that violate the relevant digital platforms' terms or policies.

Consumer law analysis

Triumph Sports Gear's ad campaign would likely contravene the provisions of section 29(1)(g) of the ACL, which prohibits a person, in connection with supplying or promoting goods, making a false or misleading representation that the goods have a certain affiliation, approval or sponsorship. The general prohibition on misleading or deceptive conduct in section 18 of the ACL may also apply.

Carlos could make a claim against Triumph Sports Gear under the ACL, seeking an injunction to prevent the ad campaign from continuing, and damages for loss suffered as a result of Triumph Sports Gear's false or misleading representations.

In addition to the ACL, Carlos may also rely on the tort of passing off to prevent Triumph Sports Gear from (or seek a remedy for) using Carlos' name, image and likeness to misrepresent the existence of an association with their tennis equipment.

Criminal law analysis

The creator of the deepfake might be prosecuted for using a carriage service to menace, harass or cause offence, or for new offences introduced in last year's *Criminal Code Amendment (Deepfake Sexual Material) Act 2024*, which targets the creation and non-consensual dissemination of sexually explicit material online, including AI generated videos. The maximum penalty for the new offence is six years imprisonment.

Defamation analysis

The laws of defamation are also well suited to addressing the reputational harm to Carlos caused by the deepfake video, particularly given that courts in Australia have a record of applying the established principles of defamation law in new online contexts.

Case study 6

AI research assistants

Case study 6

An ambitious lawyer, Jackie Davis, decides to leverage an AI-powered chatbot, Amicus Bot, to assist her in gathering relevant case law and articles that could strengthen her arguments for a dispute. After instructing Amicus Bot to locate journal articles related to her case, the chatbot returns extracts and hyperlinks from several pieces purportedly from a law journal that seem to support her position. Confident in the materials, Jackie incorporates these articles into her legal submissions to the Court, citing them as authoritative sources.

As the case progresses and the Judge's associate attempts to verify the articles cited, they discover that the articles Jackie relied on do not exist. After further investigation, the Judge concludes that the articles were fabricated by Amicus Bot. The extracts of the alleged articles, while sophisticated and relevant to the case, were entirely invented, with no traceable authorship or publication records. The hyperlinks to the articles navigates to a blank page on the journal's website. The Court calls into question the integrity of the submissions, and the matter is brought to Jackie's attention.

The Court, now sceptical of Jackie's diligence and legal professionalism, places limited weight on the submissions, damaging her client's position, and the Judge says the conduct should be considered by the local legal profession regulatory body. The Judge also makes adverse comments about Jackie's submissions in her judgment, which is published in the reported cases.

Professional ethics are at the forefront of this scenario, as lawyers are bound by strict codes of conduct designed to maintain the integrity of the legal profession. Jackie has a duty to the Court to act with honesty and integrity, and has breached her professional duties by submitting citations of articles which do not exist, and therefore misleading the Court. Despite the articles being AI hallucinations, Jackie's failure to check the legitimacy of the citations will likely mean that Jackie will face an investigation by her State or Territory legal regulatory body. Jackie's client may also bring an action for professional negligence, arguing that Jackie breached her duty of care by relying on the fabricated articles.

The NSW Supreme Court has issued a practice note regarding where the use of generative AI is acceptable for legal practitioners particularly in the context of drafting documents and summarising information.[93] The practice note sets out several areas in which practitioners should be aware of the limitations of generative AI including: the scope for hallucinations and the scope for biased or inaccurate output based on limitations in underlying datasets.[94] In relation to the preparation of written submissions, authors must verify (without the sole use of the generative AI tool) that all citations and references:

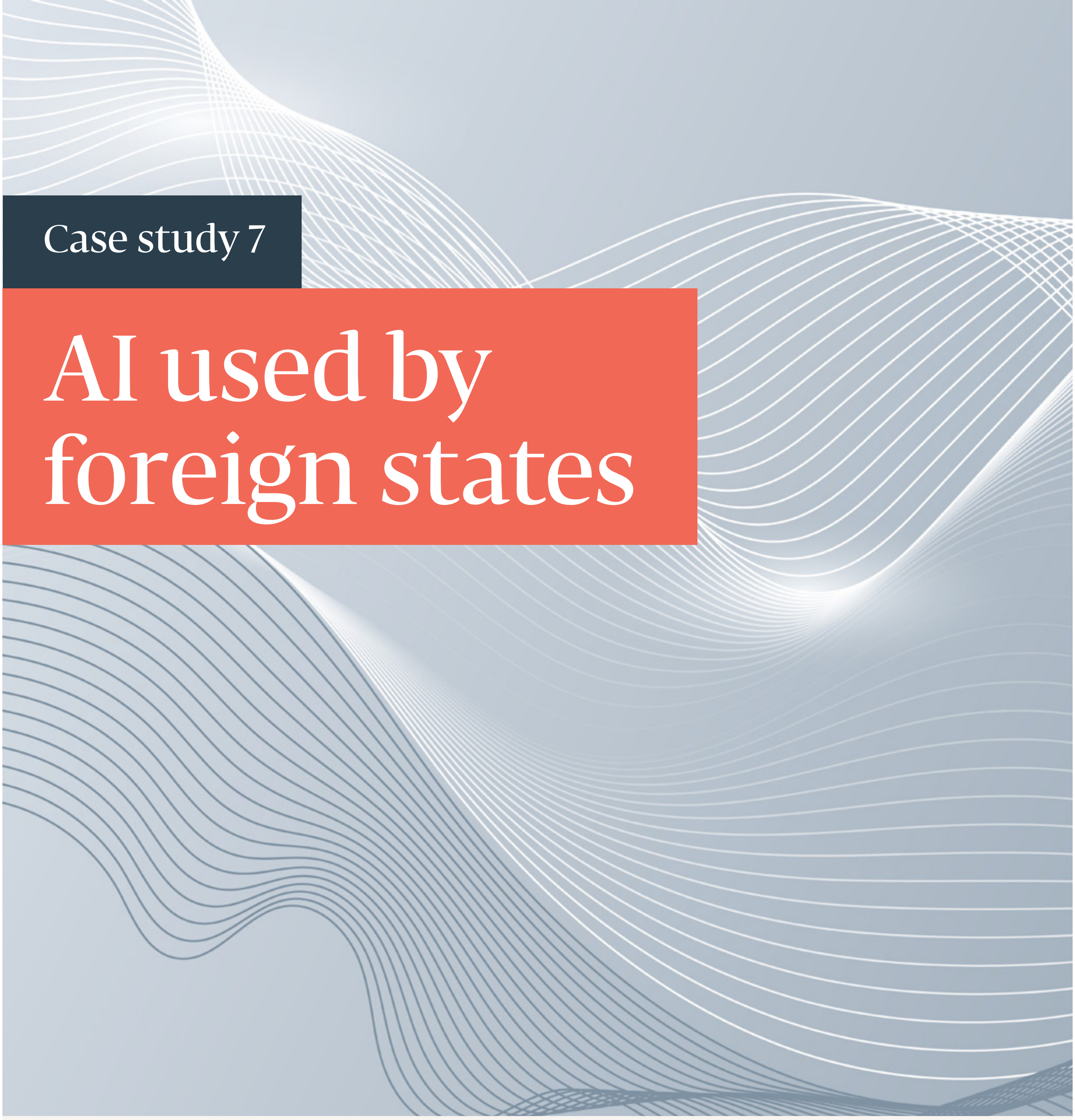
a) exist;

b) are accurate; and

c) are relevant to the proceedings.[95]

The use of any generative AI to prepare submissions, summaries or Skeleton arguments does not absolve practitioners of any professional or ethical obligations to the Court or the administration of justice.[96]

Ultimately, this scenario serves as a cautionary tale for professionals (particularly litigants) about the risks of relying on AI-generated content without proper verification and the importance of upholding the integrity of the legal profession.[97]



Case study 7

AI used by foreign states

Case study 7

In the weeks leading up to the Australian federal election, the social media website, SyncedUp, noticed an unusual spike in activity with over 300,000 new accounts emerging in the space of two weeks compared to the previous average of 4,000. Many of these accounts lacked typical user characteristics, purported to be associated with charitable organisations and were used to generate and amplify misinformation about the Government's immigration policies. These accounts, featuring profile pictures generated by AI, posted, commented and replied such that they were not easily detectable by SyncedUp's bot detection software. The activity was highly synchronised. Bots posted and reshared content at high volumes, often within seconds of each other, amplifying specific political messages and hashtags.

The bot activity was eventually linked to a foreign state government whose campaign goal was to shift public opinion on the issue of immigration in Australia by spreading misleading statistics and stories. The bots flooded feeds with low-quality but highly engaging content, making it more likely that genuine users would encounter and reshare these narratives. As a result, the overall quality of information in users' feeds declined, and authentic voices were drowned out by the volume and coordination of the bot-driven posts.

After the election, many of the bot accounts deleted their posts and deactivated, making detection and attribution more difficult for investigators.

Foreign interference

The individuals acting on behalf of the foreign state are likely to have committed one or more foreign interference offences. The relevant conduct is being initiated by those individuals. The technologies are merely the means used by the individuals.

Authorities may find it difficult to establish that the conduct was carried out for a foreign principal. The problem is exacerbated if the individuals acting on behalf of the foreign state are overseas. The use of AI in this instance assists the foreign principal in carrying out interference activities in Australia but evasion can similarly be achieved through non-AI technology. The individuals could use bots, encryption and subnet masking to conceal the fact that the conduct is being carried out on behalf of a foreign principal. The challenges in tracing the conduct back to a foreign principal exist regardless of whether AI is used.

The conduct is likely to be covert or deceptive since the individuals were posting content from accounts which purport to be associated with charitable organisations, when they were not—which is similar to the deception in *Commonwealth Director of Public Prosecutions v Duong*.[98] The use of AI to generate profile pictures and content could also amount to conduct that is deceptive. Again though, the individuals could have engaged in the same conduct without using AI. In any situation where someone pretends to be someone they are not, the element of deception will likely be made out.

The final element of whether the conduct was intended to influence Australian political processes or prejudice national security will always rest on the state of mind of the actors, and their intent or recklessness.

Our analysis leads to the proposition that the crux of the offence will continue to rest upon the conduct of a human actor. Foreign interference activities may be more easily scaled with the use of AI but the offence is still being committed by a human actor who is acting on behalf of a foreign principal.

There are always detection and enforcement challenges with foreign interference offences, and there is nothing special about AI in this regard.

Foreign influence

Whether or not the individuals acting for the foreign state need to be registered under the Foreign Influence Scheme depends on whether a person is carrying out lobbying or communications activity—this applies whether or not the person is using AI to carry out those activities. However, the person may need to disclose the use of AI in the Foreign Influence Transparency Scheme Register as part of the details on the registrable activity.

As with the foreign interference regime, it may be difficult to uncover human actors who are not complying with their obligations under the Foreign Influence Scheme.

Accordingly, the issues that arise are similar to those that arise with respect to foreign interference: the relevant obligations apply, but practical issues of identification of relevant actors and enforcement exist, regardless of whether AI is used.

Case study 8

AI use by small businesses

Case study 8

A small business owner, Sarah Chen (trading as 'Sarah's Thread & Co'), recently discovered a free AI chatbot, Unreal-IQ, which is advertised as a 'general purpose chatbot'. When accessing Unreal-IQ, users are presented with a prominent disclaimer at the top of the chat interface that states: 'Unreal-IQ is experimental and can make mistakes'. Sarah originally used the chatbot for personal use, for things like meal and recipe suggestions, planning travel itineraries and general research, but recently started using it in her business to help prepare first drafts of marketing materials and customer correspondence. Pleased with the results and cost savings, Sarah started using Unreal-IQ for business advice, such as:

- 'Can I claim the cost of a suit as a tax deduction?'.
- 'Does a customer get a refund if they change their mind about a purchase?'.

In response to the 'suit' query, Unreal-IQ advised: 'A suit can generally be claimed as a tax deduction if it is required as a uniform and bears a company logo, or is protective clothing. Suggest consulting with a registered tax agent / ATO for definitive tax advice.'

In response to the 'refund' query, Unreal-IQ advised: 'Consumers are generally not entitled to a refund if they simply change their mind. Suggest seeking legal advice regarding consumer refund obligations.'

Based on the chatbot's advice, Sarah subsequently:

- Claimed the cost of a plain business suit as a tax deduction, leading to an ATO audit and penalty.
- Refused to provide a refund to a customer whose purchased garment disintegrated in the washing machine, insisting on a store credit based on the chatbot's 'change of mind' advice. This led to a formal complaint to the State Fair Trading body, and subsequent reputational damage when the issue escalated on social media.

Sarah maintained that while the chatbot warned of errors, she relied on its 'suggestions' as a starting point, believing that the service provided a reliable general overview of Australian law for small businesses.

Consumer law analysis

In this scenario, Sarah has relied on Unreal-IQ's advice to deny a customer a refund for an obviously faulty garment, advising her that she was only entitled to a store credit. The fact that the garment disintegrated in the wash indicates that the good supplied by Sarah's Thread & Co was not of 'acceptable quality' and would very likely constitute a 'major failure' entitling the consumer to a refund (not just a store credit). By refusing the customer a refund, Sarah is potentially liable under the false, misleading or deceptive conduct provisions of the ACL and/or the consumer guarantees regime. Sarah has also relied on Unreal-IQ's advice when submitting her tax return, resulting in an ATO audit and penalty.

Sarah might try to seek compensation from the manufacturer or supplier of Unreal-IQ to cover the losses she has incurred from relying on the chatbot's answers. However, for the reasons set out below, Sarah's claim is unlikely to be successful.

Misleading or deceptive conduct / false or misleading representations

Even though Unreal-IQ is a free service, it is a service that is supplied to users in Australia, in trade or commerce, and subject to the ACL.

Unreal-IQ's answer in response to both queries have misled Sarah into error — resulting in an ATO audit and penalty in relation to the 'suit' query and a formal consumer law complaint being made in relation to the 'refund' query. That fact alone does not mean Unreal-IQ (or its manufacturer or supplier) is liable under the false, misleading or deceptive conduct or representations provisions of the ACL. Rather, it is necessary to identify the impugned conduct (i.e., a representation that is false, misleading or deceptive) and then to consider whether that conduct, considered as a whole and in context, is misleading or deceptive or likely to mislead or deceive an 'ordinary' or 'reasonable' member of the class of consumers who are likely to be affected by the conduct.

In this case, the following considerations are relevant:

- Unreal-IQ was advertised as a 'general purpose' chatbot and was not specifically designed for the purposes of providing professional business or legal advice.
- A disclaimer in the chat interface stated: 'Unreal-IQ is experimental and can make mistakes'.
- The chatbot's responses were also qualified with suggestions to seek professional advice.
- Sarah appears to have misunderstood the chatbot's response regarding the obligations to provide a refund.
- Clearer prompts, or follow-up prompts, may have produced a more useful and accurate answer.

> While disclaimers will not be sufficient in all cases to mitigate the risk of liability under the ACL, it is well established that a prominent, clear disclaimer that is in close proximity to headline statements can reduce the risk of misleading conduct.

Further, it is arguable that a reasonable user, especially a business owner, would understand that the output of a 'free' and 'experimental' chatbot may not always be accurate. While Sarah seems to acknowledge this, noting that she relied on the chatbot's output as a 'starting point', she appears to have failed to take any further steps to independently verify the information before relying on it to make business decisions.

In these circumstances, it is unlikely that the supplier of Unreal-IQ contravened the false or misleading representations, or misleading or deceptive conduct, provisions of the ACL. Sarah would remain liable for her own misleading and deceptive conduct and/or any false or misleading representations made to the customer in refusing them a refund for the faulty garment supplied by Sarah's Thread & Co.

Consumer guarantees

The consumer guarantees under Part 3-2 of the ACL apply whenever a business supplies goods or services to consumers, in trade or commerce. The relevant consumer guarantees for services include that the service will be provided with due care and skill, and that it will be fit for any disclosed purpose.

The obligation to provide services with due care and skill requires service providers to use an acceptable level of skill or technical knowledge and to take all reasonable steps to avoid causing loss or damage while providing the service. When considering whether Unreal-IQ provided its service with due care and skill, the experimental nature of the chatbot and the prominent disclaimers about its fallibility are relevant.

> The service was, by its own terms, experimental and prone to making mistakes. This reduces the expectation of absolute accuracy or professional-grade advice.

Similarly, for the guarantee of fitness for purpose, while Sarah used Unreal-IQ for business advice, its advertised purpose was for general assistance and it explicitly warned users of its experimental nature. It is arguable that a reasonable consumer would not ordinarily acquire or use this specific, free and experimental AI service for the purpose of obtaining accurate business or legal advice, especially given the clear warnings. The qualifications provided in Unreal-IQ's responses, suggesting consultation with registered tax agents or seeking legal advice, further indicate that the service itself did not purport to provide definitive professional advice.

In these circumstances, it is unlikely that the manufacturer or supplier of Unreal-IQ would be found to have breached the consumer guarantees of due care and skill or fitness for purpose in providing the erroneous business and legal advice. While Sarah would still be liable under the consumer guarantees regime for her own conduct in refusing the customer a refund for the faulty garment, she would have no right of recourse to seek compensation from the manufacturer or supplier of Unreal-IQ.

This case study highlights the importance for small business owners to exercise caution and independently verify information obtained from free or experimental AI tools, especially when making decisions that have legal or financial implications. It also highlights the benefits of broader education about the basics (and inherent limitations) of AI and appropriate and responsible use of it.

Concluding remarks

Our examination of the application of Australia's existing laws on consumer protection, employment and privacy, misinformation and disinformation, and foreign interference, in the context of the case studies in this paper, indicates that to a large extent our technology-neutral laws are capable of addressing many AI-related risks and harms.

In the course of preparing this paper, our analysis of specific AI-use cases did not reveal evidence of unique or widespread harms that would fall outside the scope of our existing laws in the targeted areas we examined. We echo the observations of the Productivity Commission that:

> 'Often, AI just provides a more efficient and effective way to accomplish things already being done (or things which could be done, but are already outlawed), and in these instances, introducing new regulations and laws to govern AI use would be both unnecessary and confusing.'[99]

In this context, the introduction of broad AI regulation on top of Australia's existing laws could create a patchwork of duplicative or inconsistent obligations. This would lead to increased compliance costs for little benefit. Regulation that goes beyond the requirements imposed by key trading partners could also have a chilling effect on the availability and/or uptake of AI systems in Australia, impeding potential productivity gains, benefits to our economy and Australia's global competitiveness. The Government is right to proceed cautiously and thoughtfully.[100]

We recognise that AI can be applied in many different ways, across many different industries and used by many different types of businesses and consumers, in high risk and low risk settings. Our paper does not seek to cover the field in this regard. We acknowledge that the risks posed by the use of AI in certain settings (e.g., healthcare, autonomous vehicles, critical infrastructure or law enforcement) are, self-evidently, much greater than those posed by the use of AI in entertainment or retail recommender systems, using chatbots to plan holidays or meals, or using an internal enterprise chatbot to help find or file documents, or understand internal policies. We also acknowledge that AI, and in particular generative AI, is still relatively new, and that new risks and harms may emerge as the technology develops further, is taken up and used in new ways.

The application of intellectual property laws to the use of copyrighted works for training AI models is another contentious and developing topic, and one that is beyond the scope of this paper. Shortly before the publication of this paper, a landmark judgment in *Bartz v Anthropic* was handed down in the US. The Court found that the use of whole books for the purposes of training AI large language models fell within the "fair use defence" under US copyright law based on the "exceedingly transformative" nature of the use.[101]

Policy development in this area needs to strike the right balance between enabling innovation and productivity gains, while providing strong safeguards against adverse outcomes. It is important that law reform that is centred on regulating for risks should be based on actual or foreseeable risks, not merely speculative risks or harms.[102]

The Government's principles for policy making stipulate that 'regulation should not be the default option for policymakers: the policy option offering the greatest net benefit should always be the recommended option'.[103] Further work is needed to clearly specify the risks and harms that are not adequately addressed through existing frameworks and need to be addressed through further regulation, including their nature and magnitude.

It is also necessary to establish that any proposed response provides a net benefit for the community, and that the net benefit is higher than what could be achieved via alternative policy responses.[104] The costs in this context are not simply the costs of administering and complying with new regulation — they include impacts on business and economic effects such as distortion of competition, reduced incentives or ability to innovate, and higher input or production costs. They also include resulting impacts on consumers such as higher prices and reduced quality and choice of products. Firms may be forced to roll out localised versions of products to Australia in order to comply with regulations, which may delay or deny Australians access to global advancements and updates associated with those products. There may also be costs to the community such as lower economic growth.

Before introducing local regulation, Australia has an opportunity to monitor how new regulations are implemented in other jurisdictions, and assess their impact on those jurisdictions' economies and global competitiveness and effectiveness in addressing relevant harms. As noted by the Productivity Commission, Australia 'is likely to be a "regulation taker" in international AI markets' in any event.[105] Given the global nature of AI supply chains, if regulatory approaches in key overseas markets, by default, regulate AI developments and outcomes in Australia, it may be unnecessary (and counterproductive) to introduce bespoke regulation in Australia that is out-of-step with overseas regulation.[106]

The case studies developed and public materials reviewed in the course of preparing this paper highlight that Government could usefully play a role in uplifting awareness and initiatives aimed at ensuring:

- businesses (particularly SMEs) deploying AI applications, supplying AI-enabled goods or services or otherwise using AI in their operations are aware of and understand their existing legal obligations and have in place robust governance arrangements.[107]
- Australian consumers (particularly older Australians who are not 'digital natives') and SMEs are educated about the basics (and inherent limitations) of AI and appropriate and responsible use of it.[108]

More effective enforcement of existing laws (including a greater willingness by regulators to run test cases) and clearer guidance from regulators are also important.

Policy development in this area needs to strike the right balance between enabling innovation and productivity gains, while providing strong safeguards against adverse outcomes. It is important that law reform that is centred on regulating for risks should be based on actual or foreseeable risks, not merely speculative risks or harms.

Annexure

Relevant Regulatory Landscape in Australia

In this section we detail the existing laws and regulations that will apply, or are likely to apply, to the use of AI in Australia, in the areas of:

- consumer law
- privacy law
- employment law
- misinformation / disinformation
- online safety
- foreign interference.

About this paper
Introduction
Case studies
Concluding remarks
Annexure

A. Consumer law

Introduction

The Australian Consumer Law (**ACL**), which sits within Schedule 2 to the *Competition and Consumer Act 2010* (**CCA**), is the principal consumer protection law in Australia. The ACL regulates relationships between suppliers, manufacturers and consumers on an economy-wide basis. It is divided into 'general protections', which establish general standards of business conduct, and 'specific protections', which provide protection for certain defined business practices. The ACL is technology-neutral. All businesses that are incorporated in Australia, carry on business in Australia or engage in relevant conduct in Australia are subject to the ACL, including those that operate online or utilise AI systems in trade or commerce.

An overview of the relevant general protections and specific protections is set out below.

Non-compliance with the ACL can result in significant pecuniary penalties, with the maximum penalty being:

a. for an individual, $2.5 million;

b. for a body corporate, the greater of:

  i. $50 million;

  ii. if the court can determine the value of the benefit that the body corporate (and any related bodies corporate) have obtained directly or indirectly and that is reasonably attributable to the commission of the offence – 3 times the value of that benefit;

  iii. if the court cannot determine the value of that benefit – 30% of the body corporate's adjusted turnover during the breach turnover period for the offence.

Note: The *Australian Securities and Investments Commission Act 2001* (**ASIC Act**) contains mirror provisions in respect of financial products and services that are not otherwise covered by the ACL. Our paper does not deal with the ASIC Act provisions.

General protections	
Misleading and deceptive conduct (sections 18 to 19)	• It is unlawful for a business to engage in conduct in trade or commerce that is misleading or deceptive, or likely to mislead or deceive. • This prohibition applies regardless of whether the business intended to mislead or deceive, or whether there is any loss or damage caused as a result of the conduct. • Statements, promises, opinions and predictions can be misleading or deceptive, as can a failure to disclose relevant information. • A key question to consider is if the overall impression of the conduct is misleading or deceptive.
Unconscionable conduct (sections 20 to 22A)	• It is unlawful for businesses to act in a way that is, in all the circumstances, considered 'unconscionable'. • Unconscionable conduct is behaviour that is so harsh, oppressive or unfair that it goes against good conscience, and beyond what is considered necessary or reasonable in the market. • The ACL provides further guidance by listing factors that may be considered when determining whether conduct is unconscionable, such as the relative bargaining power of the parties, the conduct of the parties, and whether the weaker party was under pressure or influenced in a way that impaired their ability to make informed decisions.
Unfair contract terms (sections 23 to 28A)	• It is unlawful for business to propose, use or rely on an unfair contract term in a standard form contract. • A standard form contract is one that is not negotiated. • A term is unfair if it causes a significant imbalance in the parties' rights and obligations, is not necessary to protect the legitimate interests of the party advantaged by the term, and would cause detriment to the consumer if relied upon.

Specific protections	
False or misleading representations (sections 4, 29 to 38)	• It is unlawful for a business to make false or misleading representations, including in relation to future matters, about goods or services they are supplying or promoting. • This includes false or misleading claims about the standard, quality, or value of a good or service, claims about sponsorship, approval, performance characteristics or benefits of a good or service, or the existence, exclusion of any right, remedy or guarantee. • Claims should be true, accurate and based on reasonable grounds.
Consumer guarantees (sections 51 to 68)	• Businesses are required to comply with mandatory guarantees where they supply, in trade or commerce, goods or services to consumers. • A person is taken to have purchased a good or service as 'consumer' if the amount payable for the good or service is less than $100,000 or if the goods or services are of a kind ordinarily acquired for personal, household, or domestic use or consumption. • These guarantees cannot be excluded, or contracted out of. • Guarantees for goods include that the good will be of acceptable quality (section 54) and be fit for any disclosed purpose (section 55). Guarantees for services include that the service will be supplied with due care and skill (section 60), will be fit for a particular purpose (section 61) and will be provided within a reasonable time (section 62).
Liability of manufacturers for goods with safety defects (sections 138 to 150)	• Manufacturers are liable for loss or damage caused by goods with safety defects. • A safety defect occurs where products do not meet the level of safety the public is entitled to expect. • Whether a good has a safety defect varies but factors to consider include: how and for what purpose the product has been marketed for, packaging, instructions or warnings that are included, the time the product was supplied, and what might be reasonably expected to be done with the product.
Mandatory standards (sections 104 to 108)	• Mandatory standards impose particular safety or information requirements for the legal supply of certain products in Australia. • Some products have industry standards, but these are voluntary to follow and cover other issues as well as safety. • Mandatory standards and bans are only made where evidence shows a high risk of serious injury, serious illness or death related to a product.
Product safety (sections 122 to 128 and 199 to 201)	• The ACL includes a product safety regime that provides for product recalls, mandatory safety requirements and bans. • Suppliers are expected to voluntarily recall consumer goods if they become aware that the product will or may cause injury (a failure to do so may result in the relevant Minister issuing a compulsory recall notice). • If unsafe consumer goods and/or product-related services have caused death, serious injury or illness, a supplier is required by law to give the relevant Minister (via the ACCC) written notice within two days of becoming aware of the incident.

Related law reform

During 2024 and 2025, the Government introduced legislation and proposed consultations on areas which influence how AI is regulated by consumer law.

Scams Prevention Framework (**SPF**)
In February 2025 Parliament enacted the *Scams Protection Framework Act 2025* (Cth), which attempts to combat the effects of scams on consumers. AI-enhanced technology has been used to facilitate more sophisticated scams against consumers including through phishing, deep fake technology and scam bots. The Act provides the Minister with the authority to designate businesses or services as regulated sectors including banks, telecommunication service providers and social media platforms. Whilst no entities have to date been designated under the Act, the legislation requires that designated entities adhere to six overarching principles:

3. **Govern:** Document and implement governance policies, procedures, metrics, and targets for combating scams.
4. **Prevent:** Take reasonable steps to prevent scams.
5. **Detect:** Take reasonable steps to detect scams as soon as they occur or soon afterwards.
6. **Report:** Report actionable scam intelligence to appropriate regulators (with the ACCC as the lead regulator assisted by sectorally designated regulators such as the Australian Securities and Investments Commission (**ASIC**) and the Australian Communications and Media Authority (**ACMA**)).
7. **Disrupt:** Take reasonable and proportionate steps to disrupt scam activities and prevent losses or harms arising from scams.
8. **Respond:** Have mechanisms for consumers to report scams and resolve disputes.

The considerations as to whether an entity has taken ‘reasonable steps’ will be dependent on the entity and will require businesses to consider what is ‘practical, appropriate and proportional’ based on their size, scam risk and consumer base.

Contraventions of the SPF principles or the SPF sector-specific codes can attract significant penalties based on a two-tier system with tier 1 penalties attracting penalties in excess of $50 million.

Unfair trading practices

In November 2024, Treasury proposed a consultation paper into unfair trading practices which proposes to patch practices which cause consumer harm but are not currently covered by the ACL prohibitions. The paper identifies certain problematic practices which AI may further contribute to including dark patterns and dynamic pricing. Dark patterns are design elements used in consumer interfaces that manipulate or distort consumer choices. AI may be utilised to create or enhance these webpages by personalising and targeting designs based on consumer data. Dynamic pricing or personalised pricing is a practice of varying pricing based on real-time demand including the customer’s habits and data.

The consultation paper includes a proposed general prohibition against unfair trading practices which captures conduct that:

- unreasonably distorts or manipulates the economic decision-making or behaviour of a consumer; and
- causes, or is likely to cause, material detriment (financial or otherwise) to the consumer.

In addition, Treasury has identified several specific prohibitions that it proposes to introduce. These include:

- subscription-related practices;
- drip pricing;
- dynamic pricing;
- online account requirements; and
- barriers to accessing customer support.

Consumer guarantees reform

In October 2024, a consultation paper was proposed for the design of civil prohibitions for breaches of the consumer guarantees and supplier indemnification provisions of the ACL.

The proposed amendments to the consumer guarantees penalty framework will include clearer definitions for terms like ‘acceptable quality’, ‘major failure’ and ‘reasonably durable’. Additionally, it would empower the ACCC to issue infringement notices and other penalties for non-compliance.

The paper proposes to prohibit retaliation against suppliers for requesting manufacturers indemnify for consumer guarantee failures. It also proposes to allow the ACCC to impose infringement notices on manufacturers for failure to comply with indemnification provisions.

B. Privacy law

Introduction

The Australian Privacy Principles (**APP**), which sit within Schedule 1 of the *Privacy Act 1988* (Cth) (**Privacy Act**), provide guardrails relating to the handling and management of personal information which are the cornerstone of privacy obligations in Australia. The Privacy Act recognises the need to protect the privacy of individuals through the nationally-consistent regulation of privacy and the handling of personal information. The APPs impose specific requirements on the way organisations (including most Australian Government agencies, and private sector organisations with an annual turnover of more than $3 million (**APP entities**)) collect, manage, handle, use and disclose personal information.

An overview of the relevant privacy obligations are set out below.

Note: The Privacy Act is in the process of undergoing an extensive review. The *Privacy and Other Legislation Amendment Act 2024* (Cth) received assent on 10 December 2024, and introduced the first tranche (**Tranche 1**) of privacy law reforms. Tranche 1 includes new transparency obligations regarding automated decision-making (**ADM**) including a requirement for entities to include information about the kinds of personal information used and types of decisions made in ADM in their privacy policies, and an obligation on the regulator to develop a new Children's Online Privacy Code. A second tranche (**Tranche 2**) of amendments to the Privacy Act has been proposed, with consultations underway. Tranche 2 is likely to cover a broader spectrum of issues, including a new 'fair and reasonable' requirement, consent reforms, new individual rights, small business and employee exemptions, and privacy impact assessments of high-risk activities. Other reforms relating to ADM have been proposed as a result of the Royal Commission into the Robodebt Scheme.

As part of a series of inquiries launched in December 2024, the Productivity Commission is expected to examine how Australia can support safe data access and handling through an outcomes-based approach to privacy.[109] The inquiry will look at both existing privacy laws (including Tranche 1 reforms) as well as the proposed Tranche 2 reforms. An interim report (including draft recommendations) is due August 2025, with a final report to Government due in December 2025.

There are also obligations under State and Territory privacy laws and health privacy laws, applicable to government bodies and their contractors, or to organisations handling health information. Notably, in Western Australia, the *Privacy and Responsible Information Sharing Act 2024* (WA) includes a number of new requirements similar to those proposed in Tranche 2 of the Privacy Act reforms, including in relation to ADM. Finally, certain activities are also governed by specific privacy-related laws, such as anti-spam, telemarketing, as well as surveillance devices and workplace privacy laws.

Privacy protections	
Australian Privacy Principles	
Open and transparent management of personal information and automated decision-making (APP 1)	• APP entities must take reasonable steps to implement practices, procedures and systems to ensure compliance with the Privacy Act. • Information about how an APP entity handles and manages personal information must be included in its privacy policy. • APP entities must disclose if they are using computer programs to make automated decisions using the personal information of an individual.
Anonymity and pseudonymity (APP 2)	• Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity, unless identification is required or authorised by law, or it is impracticable.

Privacy protections	
Collection of personal information (APP 3, APP 4) and notification (APP 5)	• An APP entity must not collect personal information unless the information is reasonably necessary for one or more of the entities' functions or activities. • Consent is usually required to collect sensitive information (unless certain exceptions apply). APP entities must collect information by lawful and fair means and must collect information about an individual from that individual, unless it is unreasonable or impracticable to do so. • APP entities must assess any unsolicited personal information they receive, consider if they are permitted to retain that information and if not, delete or de-identify that information. • APP entities must take reasonable steps to notify individuals, or ensure that they are aware, of certain matters (e.g. purpose of collection) at or before time of collection, or as soon as practicable after collection.
Use or disclosure of personal information (APP 6, APP 7 and APP 8)	• Generally, personal information can only be used or disclosed for the primary purpose for which it is collected. • Information can be used or disclosed for a secondary purpose with the individual's consent, or where an exception under the Privacy Act applies (e.g. if the secondary purpose is reasonably expected by the individual and it is related to the primary purpose), subject to specific rules for direct marketing and government identifiers. • APP entities must not use or disclose personal information about an individual for the purpose of direct marketing unless there is a reasonable expectation of marketing or consent has been given, there is a simple way for individuals to 'opt out', and the organisation draws attention to the ability to opt-out. • Additional restrictions apply to the use or disclosure of government related identifiers.
Quality of personal information (APP 10)	• APP entities must take reasonable steps to ensure that personal information collected is accurate, up-to-date and complete, and that personal information used or disclosed is accurate, up-to-date, complete and relevant (having regard to the purpose of that use or disclosure).
Security of personal information (APP 11)	• An APP entity must take reasonable steps to protect information from misuse, interference and loss, and unauthorised access, modification or disclosure. • 'Reasonable steps' include both technical and organisational measures.[110]
Access to and correction of personal information (APP 12, APP 13)	• APP entities must give individuals access to their personal information upon request. • APP entities must take reasonable steps to correct personal information if satisfied that (having regard to the purpose for which it is held) the information is inaccurate, out-of-date, incomplete or misleading, or if the individual requests correction.

Privacy protections	
Other privacy protections	
Notification of eligible data breaches (Privacy Act)	- An APP entity is required to investigate and report a data breach if it has reasonable grounds to believe that an unauthorised disclosure of, or access to, personal information has occurred that is likely to cause serious harm, or it is directed to do so by the Commissioner, unless an exception applies.
Serious invasions of privacy (Privacy Act)	- Individuals may take civil action for certain invasions of privacy (intrusion upon seclusion, or misuse of personal information) where there is a reasonable expectation of privacy, invasion was intentional or reckless, invasion was serious, and public interest in the plaintiff's privacy outweighs countervailing public interest.[111]
Children's Online Privacy Code (Privacy Act)	- The Office of the Australian Information Commissioner is currently required to develop an enforceable code governing online privacy for children, outlining how one or more of the APPs are to be applied or complied with in relation to the privacy of children.[112]
Doxxing (*Criminal Code Act 1995* (Cth))	- A criminal offence arises for the practice of doxxing (the publication or distribution of personal data about an individual in a way that is menacing or harassing). 'Personal data' in this context is limited to certain information that enables the individual to be identified, contacted or located.
Email or telephone marketing (*Spam Act 2003* (Cth), *Do Not Call Register Act 2006* (Cth))	- Consent is required prior to sending communication or messages of a commercial nature, by way of email or SMS. Commercial messages must include a mechanism to 'opt-out' of receiving the messages. - Direct telemarketing calls to a number listed on the Do Not Call Register are prohibited unless explicit consent is acquired or the caller is an exempt entity.
Surveillance devices and workplace monitoring (Surveillance Devices Acts, *Workplace Surveillance Act 2005* (NSW), *Workplace Privacy Act 2011* (ACT))	- Notice, consent or a warrant is required to undertake certain surveillance activities (using either listening devices, data surveillance devices, optical surveillance devices or tracking devices), unless an exception applies. - Employers are required to give employees prior notice of commencing surveillance activities. - Employers must take reasonable steps to protect surveillance records from misuse, unauthorised access or loss. Employers must take reasonable steps to destroy or de-identify any surveillance records that are no longer needed.

C. Employment law

Introduction

The increasing use of AI in Australian workplaces to manage both potential and current employees presents material risks, even though there are currently no specific laws in place to regulate this use. A primary concern is that the data used to teach and direct AI tools can contain biases, which the AI then repeats in its decisions and recommendations.

This can lead to breaches of discrimination laws throughout the entire employment lifecycle when AI tools are used for decisions from recruitment to determining pay, allocating work, monitoring performance, and even in decisions about redundancy and termination, as the AI tools could unfairly discriminate.

The risks of use of AI in the workplace has not escaped the attention of Australian legislators. In February 2025, following a lengthy inquiry into the digital transformation of workplaces, the Australian House of Representatives through its Standing Committee on Employment, Education and Training, issued *The Future of Work Report*, which made 21 recommendations on maximising the benefits of using AI in the workplace, while addressing risks and proposing new protections for employees.[113] The report highlights a range of challenges for workers and workplaces, beyond discrimination to privacy, confidentiality, transparency and fairness of decision making, and job displacement. Whether these recommendations are picked up by the Australian Government and made by the Commonwealth Parliament awaits to be seen.

For the moment, Australian employment laws will need to be leveraged for the new AI frontier. The following section will examine these potential problems in detail, considering the protections offered under the existing laws under the *Fair Work Act 2009* (Cth) (**Fair Work Act**) and Federal and State anti-discrimination legislation.

Fair Work Act

One pathway for employee claims relating to discrimination in the use of AI tools is through the 'general protections' provisions of the Fair Work Act. The operative provisions are summarised in the table below.

General protections	
Prohibition of adverse action due to protected characteristic (section 351)	An employer must not take adverse action against an employee, or prospective employee, because of the person's race, colour, sex, sexual orientation, breastfeeding, gender identity, intersex status, age, physical or mental disability, marital status, family or carer's responsibilities, subjection to family and domestic violence, pregnancy, religion, political opinion, national extraction or social origin.
Definition of adverse action (section 342)	Adverse action is defined as including: • taking action against a prospective employee by refusing to employ them or discriminating against them in the terms or conditions upon which they are offered employment; and • taking action against a current employee by dismissing them; injuring them in their employment; altering their position to their prejudice; or discriminating between them and other employees of the employer.

Accordingly, an AI tool's decision not to select a particular prospective employee as part of a recruitment process, on the basis of one of these protected attributes, would fall within the scope of the protections afforded by these provisions. That may be because, for example, the AI tool has a model that has a preference for particular attributes which may indirectly discriminate against certain groups. Similarly, relying on AI monitoring tools to inform performance review processes and termination decisions may constitute adverse action if an employee's performance is affected by a characteristic such as their physical disability but this is not considered in the AI tool's analysis. AI tools may also present risks where they are used to set remuneration and an employee is treated less favourably than another employee due to their protected characteristic. This may occur, for example, where AI tools are prompted with industry pay data and reflect any gender pay gap present within it.

Section 361 of the Fair Work Act creates a reverse onus of proof for general protections claims whereby it is presumed that an action by an employer was taken with the intent alleged by the employee, or prospective employee, unless the employer proves otherwise. This creates a high risk for employers who heavily rely on AI tools when making recruitment decisions as the reasoning processes of the AI tools may not be able to be identified, thereby making it difficult to prove that the employer had an intention other than that which was alleged. This means it is important to ensure that human oversight is involved, and recorded, in decision-making processes around recruitment so that reasonable explanations can be given as to why particular candidates were rejected from recruitment cycles.

Breaching the general protection provisions can attract the imposition of a pecuniary penalty upon the employer and other orders including reinstatement of the employee to their position or compensation for any loss they suffered because of the contravention.

Federal and State anti-discrimination regimes

Anti-discrimination laws at both the Federal and State level provide an avenue for prospective employees to raise disputes relating to the use of AI tools to reject their applications for employment. For example, these include the *Age Discrimination Act 2004* (Cth), *Disability Discrimination Act 1992 (Cth), Racial Discrimination Act 1975* (Cth) and *Sex Discrimination Act 1984* (Cth) at a Federal level and the *Anti-Discrimination Act 1977* (NSW), *Equal Opportunity Act 2010* (Vic), *Anti-Discrimination Act 1991* (Qld) and others at the State level. While these statutes are all unique, they have in common the prohibition of direct and indirect discrimination on the basis of a variety of protected characteristics.

Discrimination can be direct where a person receives less favourable treatment on the basis of an attribute protected by law (e.g. sex, age, disability, carer's responsibilities and others) compared to persons in the same or similar circumstances. In recruitment, this could arise where an AI tool prefers younger candidates rather than older candidates due to a higher proportion of young employees in the existing workforce.

Discrimination can also be indirect where a requirement, condition or practice is applied across the board, a person with a protected attribute cannot comply with it, a higher proportion of people without the attribute can comply with it, and it is not reasonable in the circumstances. For example, this could arise where an AI tool prefers candidates who have always worked full-time despite candidates who had historic caring responsibilities being unable to fulfil this criteria.

Similarly to breaches of the general protections provisions, breaches of anti-discrimination statutes can attract orders including payment of damages, imposition of penalties and requirements to reinstate employees. However, these differ depending on the jurisdiction and type of discrimination.

D. Misinformation and disinformation

Introduction

In Australia, misinformation and disinformation are not specifically regulated. Rather, various common law and legislative frameworks exist to address harmful or misleading content.

The key areas of law are:

- Australian Consumer Law (ACL);
- Tort of passing off;
- Defamation laws;
- *Criminal Code Act 1995* (Cth); and
- Australian Code of Practice on Disinformation and Misinformation.

While these areas of law provide a complementary mechanism for preventing and punishing certain acts involving the spread of misinformation and disinformation, these frameworks only form part of an effective solution.

There is no doubt that AI plays a major role in both spreading and preventing the spread of misinformation and disinformation, and while the current legal frameworks have broad applications, more targeted laws are required to regulate the spread of information online.

However, despite recent efforts by the Albanese Government to introduce legislation to Parliament to directly combat seriously harmful misinformation and disinformation on digital platforms, the *Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2024* was abandoned due to significant critiques from many legal academics, politicians and industry bodies.

In the section below, we explain a number of the legal frameworks which apply to the spread of misinformation and disinformation.

Misinformation and disinformation laws	
Australian Consumer Law	The ACL is the principal consumer protection law, and applies to all businesses operating in Australia. In the context of AI generated deepfake media content, for example, the common law of Australia does not recognise an independent cause of action to protect how a person's identity, including their name and likeness, is used. Nonetheless, a plaintiff may be able to rely on sections 18 and 29 of the ACL in a similar way. Section 29 in particular prohibits false or misleading representations that goods or services have sponsorship, approval or affiliation with a third party, when that is not the case. The Consumer Law section above provides further detail about the ACL.
Passing off	While the ACL is primarily focused on protecting consumers, the tort of passing off is concerned with preventing commercial dishonesty between traders, such as a trader making representations that falsely suggest some connection with another person's product or business. Given the broad nature of this instrument, representations made by AI systems are likely to be captured. In order to establish passing off, the following three key elements must be established:[114] **1.** the subsistence of some reputation or goodwill on the part of the plaintiff; **2.** deceptive conduct on the part of the defendant; and **3.** the existence or threat of damage to the plaintiff as a result of that conduct. The element of misrepresentation is central to the tort.

Misinformation and disinformation laws	
Defamation laws	The publication of defamatory matter is an actionable wrong at common law and by statute in each State and Territory in Australia, the purpose of which is to vindicate and protect the reputation of the person defamed. The law of defamation has historically focused on words, whether spoken or written, and is therefore well suited to address defamatory statements made by AI systems, including large language models (**LLMs**) and AI generated deepfake content. However, the tort of defamation has also been applied to images. As a result, defamation could also be used to provide a remedy in relation to the visual aspects of deepfakes or AI image generators. **Cause of action** At common law, the tort of defamation consists of the communication of a defamatory meaning 'of and concerning the plaintiff' to a person other than the plaintiff. Any communication is known as, and amounts to, publication and must itself contain, either directly or by implication, a defamatory meaning. A publication is defamatory if it tends, in the minds of ordinary reasonable people, to injure his or her reputation by either: **1.** disparaging him or her; **2.** causing others to shun or avoid him or her; or **3.** subjecting him or other to hatred, ridicule or contempt. At common law, the cause of action is complete upon the publication of a defamatory imputation and any damage may be inferred without proof of actual loss or injury to the plaintiff. In all Australian jurisdictions, except Northern Territory and Western Australia, there is now an additional, statutory element of the cause of action in defamation. To have a cause of action in defamation, the plaintiff must prove that the publication of defamatory matter has caused, or is likely to cause, serious harm to reputation.
Criminal Code	More targeted laws are being introduced to combat deepfakes used to create and share sexualised content. The *Criminal Code Amendment (Deepfake Sexual Material) Act 2024* (the **Criminal Code Amendment**) was introduced by the Australian Government as part of broader policy reforms that are aimed at strengthening online safety. The Criminal Code Amendment, which commenced on 3 September 2024, targets the creation and non-consensual dissemination of sexually explicit material online, including material created or altered using generative AI. In particular, the new offence under the Criminal Code Amendment: • targets the non-consensual sharing of sexually explicit material online, covering images and video; and • applies when a person sending the material knows or is reckless as to whether the other person consents. The maximum penalty for the offence is six years imprisonment.

Misinformation and disinformation laws	
Criminal Code (cont.)	Two aggravated offences accompany the new primary offence, one for repeat offenders with prior civil penalties under the *Online Safety Act 2021* (Cth), and another for those who created or altered the offending material, with the latter punishable by seven years imprisonment. The Criminal Code Amendment also clarifies that the form of the material is irrelevant, and includes images, videos, or audio created or altered using technology that realistically but falsely depicts another person, such as deepfakes made using generative AI.
Australian Code of Practice on Disinformation and Misinformation	The Australian Code of Practice on Disinformation and Misinformation (the **Code**) is a set of voluntary guidelines established to help combat the spread of false or misleading information on digital platforms, including social media, search engines, and other online services. It was developed by the Digital Industry Group and various stakeholders, including industry representatives, fact-checkers, and experts in the field of online information. The ACMA monitors and regulates digital platform activities under the Code. Key features of the Code include: • **Voluntary participation:** The Code is a voluntary initiative for digital platforms and online services. While platforms aren’t legally compelled to follow the code, they are encouraged to commit to the principles outlined in it. • **Responsibility of platforms:** Digital platforms, such as Facebook, Google, and Twitter, are expected to take reasonable measures to prevent the spread of misinformation and disinformation. • **Transparency and accountability:** Platforms are expected to provide more transparency regarding their efforts to combat misinformation and disinformation. This includes publishing regular reports on their actions and performance. The Code also gives particular attention to certain areas of high concern, such as public health (i.e. ensuring that health misinformation is addressed quickly and accurately) and elections (i.e. protecting democratic processes by preventing the spread of misinformation and disinformation related to elections and voting). The Australian Government has also recently published a Voluntary AI Safety Standard comprising 10 ‘guardrails’ designed to offer practical guidance to any organisation to comply with any potential future regulatory requirements in Australia and mitigate risks while leveraging the benefits of AI.

Proposed law reform

The government has increasingly scrutinised the role of tech companies and digital platforms in allowing harmful content to spread rapidly, despite many subscribing to the Code.

In response, the Australian Government introduced the *Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2024* (Cth) (**the Bill**), regulating the dissemination of misinformation and disinformation on social media platforms. Its broad aims were to:

a. impose obligations on digital communications providers in relation to the dissemination of content on a digital communications platform that contains information that is:

  i. reasonably verifiable as false, misleading or deceptive; and

  ii. reasonably likely to cause or contribute to serious harm by way of misinformation and disinformation; and

b. expand the compliance and enforcement powers of the ACMA to respond to misinformation and disinformation on 'digital communications platforms', including content aggregation services and internet search engine services (e.g., connective media services and media sharing services).

However, the Bill faced intense criticism from a wide range of bodies, including human rights organisations, church groups and libertarian groups, as well as many of the non-government members of parliament, and was ultimately withdrawn in November 2024.

The Senate Environment and Communications Legislation Committee summarised the findings of their inquiry process under four categories, which may provide insight into an improved version of the Bill being reintroduced in the future:

a. Greater transparency in ACMA's decision-making process: Many submissions received as part of the inquiry process sought greater transparency and certainty about ACMA's decision-making with respect to its code and standards-making powers.

b. A national approach to digital literacy: The Committee recommended greater efforts to improve digital literacy, including resources to help end-users to identify reliable and authoritative information sources, and to critically evaluate information they consume online.

c. Professional news content and addressing misinformation and disinformation: The Committee was of the view that whilst professional news organisations currently operate under established editorial standards and codes of practice, there remains scope to improve these frameworks.

d. Balancing freedom of expression with other human rights: The Committee received many submissions raising concerns as to whether the Bill was compatible with Australia's obligations under the International Covenant on Civil and Political Rights, particularly freedom of expression.[115] While the Committee recognised the Bill's utility in addressing the threats posed by misinformation and disinformation, there was no pathway for this Bill to pass through the Senate.

E. Online safety

Introduction

The *Online Safety Act 2021* (Cth) (**OSA**) was introduced with the aim of improving online safety for Australians by providing a comprehensive regulatory framework to address harmful online content and conduct, and introduce new powers and schemes to address cyberbullying, image-based abuse and harmful online content. There were concerns that previous frameworks were insufficiently comprehensive, and scattered through various pieces of legislation.

The OSA applies to material broadly, including material generated with the assistance of AI.

The OSA applies both to individuals that upload relevant material, and to service providers. Specifically, the OSA applies to the providers of the following services:

Online Safety Act	
Social media services	Sole or primary purpose is to enable online social interactions eg social networks, public media sharing networks, discussion forums, consumer review networks.
Age-restricted social media services	Electronic service where the sole purpose or significant purpose is to enable online social interactions, the service allows end-users to interact with other end-users, and end-users are able to post material. NB: This category only applies to Part 4A (Social media minimum age). An age-restricted social media service is not necessarily a social media service as the term is used elsewhere in the OSA.
Relevant electronic services	Email services, instant messaging services, Short Message Services (**SMS**) and Multimedia Message Services (**MMS**), chat services, online multi-player gaming services and others, including online dating services and enterprise messaging services.
App distribution services	Enable end-users to download apps eg app stores or marketplaces (but excludes links to apps and downloading of apps from third party websites).
Hosting services	Services which host stored material in Australia (e.g. services with data centres located in Australia).
Search engine services	Electronic services designed to collect, organise (index) and/or rank information on the internet in response to end-user queries and return search results to end-user queries. Excludes search functionality where content or information is generated within the platform itself and not from the internet more broadly.
Designated internet services	Allows end-users to access material using internet carriage service or delivery of service is by internet e.g. file storage services managed by end-users in Australia; websites and apps (exclusions apply).
Internet service providers	Supplies internet carriage service to the public eg retail internet service providers (**ISPs**) that supply internet carriage services (including mobile and broadband) to end users in Australia. *Note: Excludes providers of wholesale ISP services*
Equipment services	Manufacturers, suppliers, maintainers and installers of equipment used to access online services eg phones; laptops; internet-enabled devices (e.g. smart TVs, gaming consoles); immersive technologies (e.g. VR headsets); wi-fi routers.

The OSA is administered by the eSafety Commissioner, who has broad powers to investigate and respond to complaints about harmful online content, including issuing removal notices, formal warnings, infringement notices and civil penalties for non-compliance with the OSA.

The OSA is broken into the following parts:

- Basic online safety expectations (Part 4);
- Social media minimum age (Part 4A);
- Cyber bullying material targeted at an Australian child (Part 5);
- Non-consensual sharing of intimate images (Part 6);
- Cyber abuse material targeted at an Australian adult (Part 7);
- Material that depicts abhorrent violent conduct (Part 8); and
- The online content scheme (Part 9).

A high level overview of each of these parts is provided below.

Basic online safety expectations

The relevant Minister can determine basic online safety expectations for social media services, relevant electronic services and designated internet services, which service providers are expected to comply with. The basic online safety expectations are intended to set a benchmark for service providers.

The expectations are aimed at ensuring that the appearance on their service of any material in breach of the OSA is minimised by the service provider, and that there are clear and effective reporting mechanisms for end users.

The expectations include the core expectations set out in Part 3 of the OSA, together with additional expectations and examples of reasonable steps that can be taken to meet the expectations. The reasonable steps are not mandatory, they are just intended to provide guidance as to how a service provider can meet the expectations.

Online safety expectations do not impose a duty enforceable by proceedings in a Court, and the only consequence associated with breach is that the eSafety Commissioner may publish a statement regarding the fact that the service provider has breached (i.e. 'naming and shaming'). However, there are penalties for failing to comply with the reporting obligations associated with the basic online safety expectations.

There are reporting obligations in connection with the basic online safety expectations. The eSafety Commissioner may, by written notice to a service provider, require preparation of periodic reports about compliance or non-periodic reports about compliance. The Commissioner may also determine that each provider of a service has to prepare periodic or non-periodic reports about compliance.

Failure to comply with a notice or determination to provide a report can lead to a formal warning, published statement or fine of up to 500 penalty units (currently valued at $825,000 for corporations).

Social media minimum age

This is the newest inclusion in the OSA, and is not yet in force. By the end of 2025, providers of age-restricted social media platforms are expected to implement restrictions to prevent access by Australian end users under 16 years old.

Failure to do so will result in a fine of up to 30,000 penalty units ($49.5 million for corporations).

Cyberbullying material targeted at an Australian child

Cyberbullying material is defined as online communication to or about an Australian child that is likely to have the effect of seriously threatening, seriously intimidating, seriously harassing or seriously humiliating that child. For the purposes of the OSA, an Australian child is any person under the age of 18 who ordinarily lives in Australia.

The provider of a social media service, relevant electronic service or designated service about which a complaint has been made of cyberbullying material must remove the material within 24 hours of receiving a notice from the eSafety Commissioner, or the provider faces a fine of up to 500 penalty units (currently valued at $825,000 for corporations). Hosting service providers are subject to a similar obligation.

Non-consensual sharing of intimate images

Intimate images are defined as still or moving visual images showing (a) genital/anal area; (b) breasts; (c) private activity (e.g. undressing, showering, sexual activity); or (d) a person without attire of religious or cultural significance if normally worn in public. Consent to the sharing of the images must be express, voluntary and informed, or it is not valid.

The provider of a social media service, relevant electronic service or designated service about which a complaint has been made of non-consensual sharing of intimate images must remove the material within 24 hours of receiving a notice from the eSafety Commissioner, or the provider faces a fine of up to 500 penalty units (currently valued at $825,000 for corporations). Hosting service providers are subject to a similar obligation, as are individual end users who post such images.

Cyber abuse material targeted at an Australian adult

Cyber abuse material targeted at an Australian adult is material that is both (1) intended to cause serious harm, and (2) menacing, harassing or offensive in all the circumstances. Serious harm includes both serious physical and psychological harm. Serious psychological harm includes both serious psychological harm, and serious distress, but must be something beyond 'mere ordinary emotional reactions such as those of only distress, grief, fear or anger'.[116]

The provider of a social media service, relevant electronic service or designated service about which a complaint has been made of cyber abuse material must remove the material within 24 hours of receiving a notice from the eSafety Commissioner, or the provider faces a fine of up to 500 penalty units (currently valued at $825,000 for corporations). Hosting service providers are subject to a similar obligation, as are individual end users who post such material.

Material depicting abhorrent violent conduct

Provisions criminalising the upload of material depicting abhorrent violent conduct were initially introduced following the live streaming of the Christchurch mass shootings in 2019, and removal powers in relation to this material are now included in the OSA.

Abhorrent violent conduct is defined in the *Criminal Code Act 1995* (Cth) as engaging in a terrorist act, murder, attempted murder, torture, rape, or kidnap. The eSafety Commissioner can issue a notice requesting an internet service provider to disable access to material which promotes, incites, instructs or depicts abhorrent violent conduct (a **blocking request**). Alternatively, the eSafety Commissioner can issue a notice requiring the blocking of this material by the internet service provider (a **blocking notice**).

Failure to comply with a blocking notice can result in a fine of up to 500 penalty units (currently valued at $825,000 for corporations).

However, there are defences available for material for academic research, news reporting and for public officials.

Online content scheme

The Online Content Scheme deals with the availability of class 1 and class 2 material over the internet.

Class 2 material is material which would be classified as X18+ or R18+ by the Australian Classification Board. R18+ material is material legally restricted to adults 18 and over, which contains content that may be offensive to sections of the population. X18+ material is material which contains sexually explicit activity including actual sexual intercourse or other sexual activity between consenting adults.

Class 1 material is material that would be **refused** classification by the Australian Classification Board: this is material which is outside generally accepted community standards, and exceeds what would be included in the X18+ rating. Material that is refused classification cannot be sold in Australia.

Class 1 material is then divided into three further subcategories:

1. Class 1A material: child sexual exploitation material, pro-terror material, and extreme crime and violence material;
2. Class 1B material: crime and violence material and drug-related material; and
3. Class 1C material: particular online pornography which either:
    - a. depicts, expresses or otherwise deals with matters of sex in such a way that the material offends against the standards of morality, decency and propriety generally accepted by reasonable adults to the extent that such material should not be classified; or
    - a. includes or contains gratuitous, exploitative or offensive depictions of (i) sexual activity accompanied by fetishes or practices which are offensive or abhorrent; or (ii) incest fantasies or other fantasies which are offensive or abhorrent.

A service provider (social media service, relevant electronic service, designated internet service or hosting service) must remove or cease hosting class 1 material within 24 hours (or longer, if allowed by the Commissioner) of being issued with a removal notice by the eSafety Commissioner. Failure to comply with a removal notice can result in a fine of up to 500 penalty units (currently valued at $825,000 for corporations).

There are similar removal notice provisions in respect of class 2 material, but these provisions only apply if the service is provided from Australia or the material is hosted in Australia. The eSafety Commissioner can also issue a notice requiring certain types of class 2 material be subject to a restricted access system (i.e. not available to users under 18).

Search engine providers may also be issued with a link deletion notice, requiring them to remove a link to class 1 material within 24 hours. Failure to comply with a link deletion notice can result in a fine of up to 500 penalty units (currently valued at $825,000 for corporations). Similarly, app distribution service providers can be required to remove apps which facilitate the posting of class 1 material.

Industry codes and standards

The OSA also provides for the introduction of industry codes (prepared by industry stakeholders and registered with the eSafety Commissioner) or industry schemes (prepared by the eSafety Commissioner, in the event the industry code is rejected) in respect of the Online Content Scheme. These codes and standards create minimum requirements for service providers to meet in respect of class 1 and class 2 material.

Failure to comply with an industry code or standard results in a penalty of up to 30,000 penalty units ($49.5 million for corporations).

Currently, there are the following codes and standards in place in respect of class 1A and class 1B material:

- Social Media Services Online Safety Code;
- App Distribution Services Online Safety Code;
- Hosting Services Online Safety Code;
- Equipment Online Safety Code;
- Internet Search Engine Services Online Safety Code;
- Relevant Electronic Services — Class 1A and Class 1B Material Industry Standard 2024; and
- Designated Internet Services — Class 1A and Class 1B Material Industry Standard 2024.

The above codes are also subject to head terms, which apply to all of the codes (but not the standards).

The codes and standards require service providers to undertake risk assessments, proactively deal with class 1A and class 1B material, handle complaints, take action against users uploading violating materials, and make relevant information available to end users.

Codes in relation to class 1C and class 2 material are currently in place in relation to search engines, hosting services and internet service providers. These codes require services providers to adopt measures to protect minors from access and exposure to pornography, violence and material promoting suicide, self-harm and eating disorders. Further codes for other online sectors are currently in development, and are expected in late 2025.

F. Foreign interference and influence

Introduction

Foreign interference has been in the global spotlight since the 2016 US Presidential election. It was reported, controversially, that Russia used social media accounts and interest groups to sow discord in the US political system, in addition to hacking and leaking data that was politically sensitive.[117] Since that time, there have been increasing concerns that foreign actors engaging in such conduct, which is sometimes termed 'information warfare', could influence voter decisions, diminish public confidence in democratic processes and create unrest.

In Australia, concern about foreign interference has attracted political, legislative and regulatory attention, including with reference to the impact of AI. In 2017, then Prime Minister Malcolm Turnbull declared during his second reading speech for the *National Security Legislation Amendment (Espionage and Foreign Interference) Bill* 2017, 'We are witnessing the mass production, the democratisation if you like, of disinformation... And now these methodologies have been turbocharged by cyber'.[118] Earlier this year, the Director-General of Australian Security Intelligence Organisation (**ASIO**), Mike Burgess, warned 'Espionage and foreign interference are already at extreme levels and we anticipate they will only intensify...espionage and foreign interference will be enabled by advances in technology, particularly Artificial Intelligence'.[119]

This had led to two significant law reforms. The first criminalised certain conduct by way of foreign interference, which is essentially covert or deceptive foreign activity directed to influencing Australian political processes, supporting foreign intelligence or prejudicing Australia's national security. The second sought to regulate activities on behalf of a foreign actor which are overt, by requiring registration and other transparency measures.

Foreign interference was criminalised in 2018 by the *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* (Cth), which introduced offences of foreign interference into section 92 of the Criminal Code. The offences may apply in respect of covert activity carried out by, or on behalf of, a foreign actor, which is coercive or deceptive, and is done with the intention of, or being reckless as to whether it will influence government or the political process, influence the exercise of a democratic right or duty, support foreign intelligence activities or prejudice national security. There may be practical difficulties in enforcing the offence against foreign actors overseas — which we explore further in this paper.

The main offence in section 92.2 of the Criminal Code (intentional foreign interference generally) applies where a person engages in covert or deceptive conduct for a foreign principal that is intended to influence Australian political processes or prejudice national security. The maximum penalty is 20 years imprisonment.

There are also three related offences. There is an offence of intentional interference involving a targeted person. This occurs where a person engages in conduct secretly for a foreign principal that is intended to influence another person in relation to Australian political or governmental processes (20 years imprisonment maximum penalty).

There are then versions of the above two offences, which only require recklessness, rather than intention. These attract 15 years imprisonment maximum penalty.

The primary offence of intentional foreign interference generally requires:

1. conduct for a foreign principal;
2. which is covert or deceptive; and
3. which is intended to influence Australian political processes or prejudice national security.

The offences apply to conduct outside Australia if the result of the activity occurs in part or in whole in Australia, or conduct carried out by an Australian citizen or resident.[120]

For a foreign principal

A foreign principal includes the government of a foreign country or part of a foreign country, a foreign political organisation and a company which is majority controlled by a foreign government. Because the offence is directed to conduct by government or politically linked foreign bodies, enforcement presents inherent challenges. Where the actors are offshore, investigation to establish the identity of the foreign actor may be problematic.

For example, fake social media accounts could be set up to carry out conduct at the behest of a foreign principal. It would be difficult for Australian authorities on their own, to identify the foreign principal ultimately controlling those accounts. Encryption technologies can be used to mask the involvement of a foreign principal. Those technologies, which have been readily available for some years now, can come in many forms and be as basic as using anonymous or masked identities over an online messaging service. Even if that can be overcome, authorities will also face a practical difficulty in enforcing the offence against foreign actors or principals who are overseas. These are inherent challenges in detecting and enforcing the legislation, regardless of any use of AI.

Covert or deceptive

Deceptive includes a deception as to the intentions of the person using the deception or any other person, as well as conduct by a person that causes a computer, machine or electronic device to make a response that the person is not authorised to cause it to do. Covert is not defined within the Criminal Code but likely takes its ordinary meaning of things that are not openly acknowledged or displayed. This element of the offence would equally apply to any technology capable of masking the identity of an actor carrying out foreign interference activities.

In *Zhang v Commissioner of Police* [2021] HCA 16, when considering whether search warrants were validly issued on the basis of suspected contraventions of foreign interference offences, the High Court found that the word 'covert' is 'on any view susceptible of a range of arguable applications involving a spectrum of arguable shades of meaning'. The search warrants issued by the Commissioner of Police stated that the accused had engaged an elected Australian official 'through a private social media chat group' on behalf of a foreign principal. The accused sought to have the warrants quashed by the High Court but was unsuccessful. While the question was not fully considered by the High Court, it is notable that 'private social media chat groups' were sufficient grounds for the accused's conduct to be considered potentially covert or deceptive for the purpose of the search warrants.

Intended to influence Australian political processes or prejudice national security

This element is capable of being inferred from conduct which has influenced Australia's voting process, the actions or views of members of parliament or damage Australia's national security. In *Commonwealth Director of Public Prosecutions v Duong* [2024] VCC 182, the defendant was convicted of foreign interference offences for intending to solicit a Federal Minister to influence political or governmental processes in Australia to the advantage of the Chinese Communist Party.[121]

Critically, it is integral to the offence (and to the lesser offence based on recklessness), that the defendant has the relevant state of mind. The detection and enforcement challenges where the actor is outside Australia, identified above, also arise in relation to this element.

Foreign influence

While foreign interference is an offence, the existing national security legislation recognised that foreign influence can occur legitimately, for example as part of diplomacy, if it is carried out in an open and transparent manner. Foreign influence is regulated by ***the Foreign Influence Transparency Scheme Act 2018 (Cth)*** (**the FIT Scheme Act**). The High Court has said:

> Even when the purpose of the foreign influence is not to damage or destabilise Australia, if left undisclosed it can impede the ability of decision-makers in Australia, and the Australian public, to make informed decisions because it can conceal the nature of the competing interests at play.... transparency of foreign influence can contribute to the effective functioning and accountability of Australian government institutions and help protect their integrity by reducing the risk that foreign influence will result in foreign interests prevailing over domestic interests by ensuring that the Australian public can assess the nature, level and extent of foreign influence in respect of particular decisions or processes accurately.[122]

The FIT Scheme Act has been the subject of a review by the Parliamentary Joint Committee on Intelligence and Security, which reported in 2024. The report identified significant flaws in the Scheme and recommended significant reform. The government has accepted this recommendation. As the committee's recommendations were unanimous, it is likely reforms will be implemented.[123]

The FIT Scheme Act applies to persons who undertake certain activities in Australia, on behalf of a foreign principal, for the purpose of political or governmental influence. There is no requirement for the person to be present in Australia while carrying out the activities. The offence of not registering under the FIT Scheme Act applies to activities carried out by persons outside of Australia if the result of the activity occurs in part or in whole in Australia.[124]

It requires such persons to be on a public register for the purposes of transparency. It does not prohibit the activities. The activities are:

- Lobbying MPs or general political lobbying — includes communicating with a person or group of persons for the purpose of influencing any process decision or outcome whilst representing the interests of another person;
- communications activity — occurs if a person 'communicates or distributes information or material to the public or a section of the public' or produces information for such a purpose. This is subject to an exception where the activity is in the ordinary course of the person's business, and the information or material is produced by another person and their identity is disclosed (or, if they produced it for another person, that person's identity is disclosed); and
- disbursement activity (ie payments or providing things of value).

A person who registers must provide on the register a description of the relevant activities.[125] If the use of AI is inherent to the activity, this may mean its use must be expressly disclosed.

Endnotes

1 Annexure to this paper provides more detail regarding the existing laws and regulations in each of these areas that will apply, or are likely to apply, to the use of AI in Australia.

2 ASIC, 'Beware the Gap: Governance Arrangements in the Face of AI Innovation' (Report, October 2024). The report examined the ways Australian financial services and credit licensees are implementing AI where it impacts consumers and found there is the potential for a governance gap.

3 For example, a key pillar of the Singapore government's National AI Strategy is AI talent and education: to further help Singaporeans understand the fundamentals and applications of AI, be it in their workplace or daily lives, SkillsFuture Singapore has partnered with major technology partners, to offer a SkillsFuture for Digital Workplace program with relevant AI content, which is subsidised by the Singapore government, and the Singapore government has funded free AI literacy courses for the general public. See Smart Nation Singapore, 'National Artificial Intelligence Strategy - Advancing our Smart Nation Journey' (Report, November 2019) and AI Singapore 'AI for Everyone' (Webpage, accessed June 2025). The National Artificial Intelligence Centre's report highlights the need for a whole-of-society program of high-quality AI literacy: Australian Department of Industry, Sciences and Resources and National Artificial Intelligence Centre, 'Australia's Artificial Intelligence Ecosystem: Growth and Opportunities' (Report, June 2025) p. 64.

4 Jacob Turner, 'Robot Rules: Regulating Artificial Intelligence' (Book, Palgrave Macmillan Cham, 2018) p. 28.

5 Organisation for Economic Co-operation and Development AI Policy Observatory ('OECD.AI'), 'What is AI? Can you make a clear distinction between AI and non-AI systems?' (Webpage, 6 March 2024).

6 Australian Department of Industry, Science and Resources, 'The Bletchley Declaration by Countries Attending the AI Safety Summit, 1–2 November 2023' (Media Release, 2 November 2023); Australian Productivity Commission, 'Making the Most of the AI Opportunity - Research Paper 1' (Report, January 2024) p. 4; Australian Department of Industry, Science and Resources, 'Safe and Responsible AI in Australia Consultation: Australian Government's Interim Response' (Report, 17 January 2024) pp. 8-9.

7 Some of these benefits are discussed in Australian Productivity Commission 'Making the Most of the AI Opportunity - Research Paper 1' (Report, January 2024); Google, 'An AI Opportunity Agenda for Australia' (Report, 27 May 2024) and the Australian Department of Industry, Sciences and Resources and National Artificial Intelligence Centre, 'Australia's Artificial Intelligence Ecosystem: Growth and Opportunities' (Report, June 2025). The National Artificial Intelligence Centre's Report references some global and local examples: DeepMind's AlphaFold and Isomorphic Labs' newer protein-structure prediction tools have transformed drug discovery pipelines; in Australia - SwarmFarm Robotics opened a major manufacturing hub in Queensland in 2024 to scale autonomous farm machines that reduce chemical use and boost productivity; Heidi Health offers an AI-powered medical scribe that transcribes patient consultations into clinical notes, case histories and other medical documents; Monash University launched a generative AI tool in 2025 designed to simulate scientific processes and accelerate research breakthroughs; and Harrison.ai is developing AI solutions for medical diagnostics. Rio Tinto has implemented AI in its automated rail network, creating the world's largest robotic rail operation (it's AI-powered Mine Automation System operates across 98% of mining sites, reducing Tier 1 safety incidents by 50%).

8 Australian Productivity Commission, 'Making the Most of the AI Opportunity - Research Paper 2: The Challenges of Regulating AI' (Report, January 2024) p. 2.

9 For example, Dario Amodei, CEO of AI firm Anthropic has suggested that AI could wipe out half of all entry-level white-collar jobs and spike unemployment to 10-20% in the next 1-5 years (see Jim VandeHei and Mike Allen, 'Behind the Curtain: A White-collar Bloodbath' (News Article, Axios, 28 May 2025)); Amazon's CEO Andy Jassy, CBA's CEO Matt Comyn and Telstra's CEO Vicky Brady have each warned their workforces will be smaller by the end of the decade, (see Paul Smith, 'Amazon CEO Warns White-collar Staff That Their Jobs are on the Line' (News Article, AFR, 18 June 2025)). Others are more optimistic about job creation, see eg, Mckinsey Global Institute, 'Jobs Lost, Jobs Gained: What the Future of Work Will Mean for Jobs, Skills, and Wages' (Article, 16 July 2024)); 19% of economists surveyed by the World Economic Forum expect net job gains and 33% predict no change (as reported in World Economic Forum, 'Chief Economists Outlook' (Report, May 2025), p. 28); the Tech Council of Australia estimates development and adoption of AI in Australia could create up to 200,000 jobs by 2030 (Tech Council of Australia, 'TCA Statement on the Government's National AI Capability Plan' (29 January 2025)) and the Business Council of Australia is also optimistic that AI will not result in mass job displacement (Business Council of Australia, 'Accelerating Australia's AI Agenda' (Report, June 2025) p. 19). The National Artificial Intelligence Centre observes in that '[o]ngoing monitoring is needed to understand workforce trends, job displacement risks, and how well educational and training programs align with market needs' (see Australian Department of Industry, Sciences and Resources and National Artificial Intelligence Centre, 'Australia's Artificial Intelligence Ecosystem: Growth and Opportunities' (Report, June 2025) p. 62; Jobs and Skills Australia is undertaking a capacity study on the implications of generative AI for the Australian labour market, workforce planning and associated needs within the national skills system (Jobs and Skills Australia, 'Generative Artificial Intelligence Capacity Study' (Webpage, accessed June 2025)).

10 Senate Select Committee, 'Select Committee on Adopting Artificial Intelligence (AI): Final Report' (Report, November 2024) Chapter 6 — Impacts of AI on the Environment.

11 See eg, Kristalina Georgieva 'AI Will Transform the Global Economy. Let's Make Sure it Benefits Humanity' (IMF Blog, 14 January 2024) and International Monetary Fund, 'IMF Staff Discussion Notes — Gen-AI: Artificial Intelligence and the Future of Work' (Report, 14 January 2024) p. 19.

12 Future Matters Centre of Excellence, 'Harnessing AI: Insights and Innovation in Financial Services' (Report, October 2024) p. 7; OECD, 'Venture Capital Investments in Artificial Intelligence' (Report, September 2021); European Commission, 'Commission

Launches AI Innovation Package to Support Artificial Intelligence and SMEs' (Webpage, 24 January 2024).

[13] CSIRO, 'Artificial Intelligence Roadmap' (Webpage, 24 August 2022). Others have estimated the value of AI to the global economy at between $5 trillion and over $20 trillion. See PricewaterhouseCoopers, 'Sizing the Prize' (Report, 2017) and UNCTAD, 'Technology and Innovation Report' (Report, April 2025).

[14] World Economic Forum, 'Chief Economists Outlook' (Report, May 2025) p. 27.

[15] Australian Department of Industry, Science and Resources, 'Safe and Responsible AI in Australia Consultation - Australian Government's Interim Response' (Report, January 2024); McKinsey & Company, 'Proceed with Caution: Three Questions for Australian Governments to Answer as they Consider Gen AI' (Webpage, 17 March 2024); Microsoft and Tech Council of Australia 'Australia's Generative AI Opportunity' (Report, July 2023) p. 3, estimates generative AI could add up to $115 billion in productivity gains to the Australian economy by 2030 (a 5% uplift in GDP).

[16] OECD.AI, 'A sharp increase in AI-related venture capitalist investments could transform global economies and shape the future of artificial intelligence' (Webpage, 2021); Our World in Data, 'Annual Global Corporate investment in artificial intelligence, by type' (Webpage, 2022); Australian Department of Industry, Sciences and Resources and National Artificial Intelligence Centre, 'Australia's Artificial Intelligence Ecosystem: Growth and Opportunities' (Report, June 2025) p. 8.

[17] Australian Government Productivity Commission, '5-year Productivity Inquiry: Australia's Data and Digital Dividend' (Report, 7 February 2023) Vol. 4, p. 11.

[18] See Mel Silva, 'AI Adoption in Australia: New Survey Reveals Increased Use & Belief in Potential' (Webpage, Google Blog, 22 January 2025).

[19] Australian Productivity Commission, 'Making the Most of the AI Opportunity - Research Paper 1' (January 2024) p. 8.

[20] ASIC, 'Beware the Gap: Governance Arrangements in the Face of AI Innovation' (Report, October 2024) p. 11—12.

[21] Australian Department of Industry, Sciences and Resources and National Artificial Intelligence Centre, 'Australia's Artificial Intelligence Ecosystem: Growth and Opportunities' (Report, June 2025) p. 6, citing NAIC and Fifth Quadrant, 'SME AI pulse: Tracking the adoption & perception of AI in Australian Business' (Report, Q1 2025); AiGroup 'Technology Adoption in Australian Industry: Commercial, workforce and regulatory drivers' (Report, October 2024); Ben Abbott 'Australian Enterprises Coming 4th in 2024 Global Survey of Generative AI Usage' (Webpage, TechRepublic, 9 August 2024).

[22] Australian Department of Industry, Sciences and Resources and National Artificial Intelligence Centre, 'Australia's Artificial Intelligence Ecosystem: Growth and Opportunities' (Report, June 2025) p. 6, citing Governance Institute of Australia, '2025 AI Deployment and Governance Survey Report' (Report, 2025).

[23] ACCC, 'Digital Platform Services Inquiry - Final Report' (Report, March 2025) p. 260.

[24] Ibid p. 265.

[25] Australian Productivity Commission, 'Making the Most of the AI Opportunity - Research Paper 1' (Report, January 2024) p. 9.

[26] As noted above, the authors acknowledge the relevance and application of other areas of law to AI, including competition law, copyright law, negligence and sector-specific and profession-specific requirements; however, they are beyond the scope of this paper.

[27] The Singapore Government is providing up to a 70% subsidy for law firms to use generative AI (Singaporean Ministry of Law, 'Enhanced Productivity for Law Firms in Singapore with the Integration of Microsoft Copilot into the Legal Technology Platform' (Media Release, 11 September 2024)).

[28] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 on Artificial Intelligence and Amending Certain Union Legislative Acts (Artificial Intelligence Act) [2024] OJ L 12.7.2024, 1.

[29] For example, *FAA Reauthorization Act of 2018*, HR 302, 115th Congress (2017-2018); *National Artificial Intelligence Initiative Act of 2020*, HR 6216, 116th Congress (2019-2020).

[30] *Defending Democracy from Deepfake Deception Act of 2024,* AB 2655; *Use of Likeness: Digital Replica Act,* AB 1836; *California AI Transparency Act,* SB 942; *Health Care Services: Artificial Intelligence Act,* AB 3030.

[31] State of Utah, *Artificial Intelligence Amendments 2024 General Session*, S.B. 149, 2024.

[32] Colo. Rev. Stat. §6-1-1701 to 6-1-1707 (2024-25).

[33] Stanford HAI, 'Artificial Intelligence Index Report 2025' (Report, 2025) p. 341.

[34] PDPC, 'Model Artificial Intelligence Governance Framework' (Guideline, 21 January 2020).

[35] The principles are (a) not infringing on fundamental human rights; (b) safety; (c) fairness; (d) privacy protection; (e) security; (f) transparency; (g) accountability; (h) education / literary; (i) ensuring fair competition; and (j) promoting innovation and considering interconnectivity and interoperability.

[36] Mario Draghi, 'The Future of European Competitiveness - Part A: A Competitiveness Strategy for Europe' (Report, September 2024) p. 6-9.

[37] Raluca Csernatoni, 'The EU's AI Power Play: Between Deregulation and Innovation' (Report, Carnegie Europe, 20 May 2025) p. 3.

[38] See eg, Australian Department of Industry, Science and Resources, 'Safe and Responsible AI in Australia Consultation: Australian Government's Interim Response' (Report, 17 January 2024); Stephen Jones, 'Albanese Government Opens Consultation on review of Artificial Intelligence and the Australian Consumer Law' (Media Release, 15 October 2024).

[39] Jim Chalmers, 'Terms of reference: Creating a More Dynamic and Resilient Economy' (Productivity Commission, 13 December 2024); Australian Productivity Commission, 'Harnassing Data and Digital Technology: Enable AI's Productivity Potential' (Webpage, accessed June 2025).

[40] Australian Productivity Commission, ‘Making the Most of the AI Opportunity - Research Paper 1’ (Report, January 2024) p.13.

[41] Australian Department of Industry, Science and Resources, ‘Australia’s AI Ethics Principles’ (Webpage, accessed June 2025).

[42] Australian Department of Industry, Science and Resources, ‘Voluntary AI Safety Standard’ (Guideline, August 2024).

[43] Australian Department of Industry, Science and Resources, ‘Safe and Responsible AI in Australia Consultation - Australian Government’s Interim Response’ (Report, 17 January 2024); Australian Department of Industry, Science and Resources, ‘Voluntary AI Safety Standard v2 Consultations: Expressions of Interest’ (Webpage, accessed June 2025).

[44] In this paper, an AI developer is a person or organisation that creates an AI model or system with the intent to deploy it or provide it to others. An AI deployer is a person or organisation that puts into service an AI system, whether it has developed that system totally or partially.

[45] Australian Government Digital Transformation Agency, ‘Policy for the Responsible Use of AI in Government’ (Guideline, September 2024).

[46] Australian Government Digital Transformation Agency, ‘Cyber Risk Model Clauses’ (Guideline, March 2025).

[47] ASIC, ‘ASIC Alleges IAG Misled Home Insurance Customers on Pricing Discounts’ (Media Release, 25 August 2023).

[48] *Australian Competition and Consumer Commission v Trivago N.V.* [2020] FCA 16.

[49] OAIC, ‘Bunnings Breached Australian’s Privacy with Facial Recognition Tool’ (Media Release, 19 November 2024). Bunnings is challenging the decision.

[50] See the eSafety Commissioner’s Register of Industry Codes and Industry Standards for Online Safety (Webpage, accessed June 2025) and Information About Industry Codes (Webpage accessed June 2025).

[51] World Benchmarking Alliance, ‘Ethical AI Collective Impact Coalition Dataset’ (Report, 20 September 2024).

[52] Google, ‘Responsible AI Progress Report’ (Report, February 2025). Earlier reports are available here.

[53] Open AI, ‘Open AI Charter’ (Webpage, accessed June 2025).

[54] Microsoft, ‘Microsoft Responsible AI: Principles and Approach’ (Webpage, accessed June 2025).

[55] Samsung, ‘AI Ethics: Samsung Electronics’ Commitment to AI Ethics Principles’ (Webpage, accessed June 2025).

[56] Paula Goldman, ‘How Salesforce Shapes Ethical AI in the Agent Era’ (Media Release, Salesforce, 28 October 2024).

[57] IBM, ‘IBM’s Principles for Trust and Transparency’ (Webpage, accessed June 2025); IBM, ‘What is AI Ethics?’ (Webpage, accessed June 2025); IBM, ‘IBM Consulting Unveils Center for Excellence for Generative AI’ (Webpage accessed June 2025).

[58] OECD.AI, ‘G7 Reporting Framework – Hiroshima AI Process (HAIP) International Code of Conduct for Organizations Developing Advanced AI Systems’ (Webpage, accessed June 2025).

[59] *Australian Competition and Consumer Commission v Valve Corp* (No 3) (2016) 337 ALR 647, 687-8.

[60] Ibid 687, citing *Bray v F Hoffman-La Roche Ltd* (2002) 190 ALR 1, 15-6.

[61] *Hornsby Building Information Centre Pty Ltd v Sydney Building Information Centre Ltd* (1978) 140 CLR 216; *Parkdale Custom Built Furniture Pty Ltd v Puxu Pty Ltd* 1982] HCA 44; *Yorke v Lucas* [1985] HCA 65.

[62] ACL ss 18, 29.

[63] *Australian Competition and Consumer Commission v Sony Interactive Entertainment Network Europe Ltd and Another* (2020) 381 ALR 531.

[64] *Moffatt v Air Canada* (2024) BCCRT 149.

[65] *Australian Competition and Consumer Commission v iSelect Ltd* [2020] FCA 1523; Australian Competition and Consumer Commission, ‘iSelect to Pay $8.5 Million for Misleading Consumers Comparing Energy Plans’ (Media Release No 211/20, 8 October 2020).

[66] *Australian Competition and Consumer Commission v Master Wealth Control* (Penalty) [2024] FCA 795.

[67] ACL s 236; Damages are calculated based on loss suffered from reliance rather than expectation: *Gates v City Mutual Life Assurance Society Ltd* (1986) 160 CLR 1, 14–15.

[68] ACL s 3 (definition of ‘consumer’).

[69] ACL ss 60, 61.

[70] It could also be a result of the chatbot hallucinating, or erroneous inputs leading to erroneous outputs.

[71] It can be distinguished from dynamic or ‘surge’ pricing, which adjusts based on external market conditions (eg low supply, high demand). For example, dynamic pricing is common in the travel industry with theme parks often charging different admission fees depending on the time of year, hotels offering lower rates for their rooms during ‘off-season’ and airlines charging different fares depending on seat availability (see Melissa Kravitz Hoeffner, ‘How Does Dynamic Pricing for Airlines Affect Your Travels’ (News Article, Forbes, 11 March 2024). Following the release of the Oasis Reunion Tour, the European Commission and the UK Competition and Markets Authority announced reviews into dynamic pricing practices. UK Competition and Markets Authority, ‘Dynamic Pricing Project’ (Webpage, accessed June 2025); Pierfrancesco Maran, Brando Benifei, ‘“Dynamic pricing” Practices in the EU and Protecting the Rights of EU Consumers’ (Webpage, European Parliament, 5 September 2024); Didier Reynders, ‘Answer given by Mr Reynders on Behalf of the European Commission’ (Webpage, European Parliament, 5 November 2024).

[72] Dr Son Tan Nguyen, ‘Algorithmic Price Personalisation: Everything You Need to Know’ (Article, *LSJ Online*, 7 February 2025) pp.1-2; Dr Son Tan Nguyen, ‘Algorithmic price personalisation and consumer protection in Australia’ (2024) 31 *CCLJ* 80.

[73] UK Competition and Markets Authority, ‘Evidence Review of Online Choice Architecture and Consumer and Competition Harm’ (Report, 5 April 2022). There are various examples highlighting the fairness and privacy concerns that are arising as a result of this type of conduct. In 2015, Disneyland Paris was investigated by European regulators in relation to alleged price discrimination whereby it charged varying prices based on consumer country of residence (Jim Brunsden and Duncan Robinson, ‘Disneyland Paris Ditches Pricing Policy’ (News Article, Financial Times, 16 April 2016)). AirAsia Bhd reportedly used machine learning to understand passengers’ willingness to pay increased baggage fees (Jamie Freed, ‘AirAsia Testing Personalised Baggage Pricing, Eyes More Add-on Revenues’ (News Article, Reuters, 16 November 2017). Uber has revealed that it studies users and circumstances in which users would be willing to pay more for a ride, for example someone travelling from a wealthy neighbourhood or a user with low phone battery (Bloomberg, ‘Uber Starts Charging What It Thinks Your Willing to Pay’ (News Article, 19 May 2017); Ryan Calo and Alex Rosenblat, ‘The Taking Economy: Uber, Information and Power’ (2017) 117 *Columbia Law Review* 1623, 1630). A 2022 study found that online dating platform, Tinder, uses a personalised pricing algorithm to charge older users more than younger users for the

same service (Mozilla, 'New Research: Tinder's Opaque, Unfair Pricing Algorithm Can Charge Users Up to Five-Times More For Same Service' (Media Release, 8 February 2022)).

[74] Dr Son Tan Nguyen, 'Algorithmic Price Personalisation: Everything You Need to Know' (Article, *LSJ Online*, 7 February 2025) p. 2.

[75] It is well-established that silence or omissions may constitute misleading or deceptive conduct under section 18 of the ACL.

[76] Australian Treasury, 'Unfair trading practices: Consultation on the Design of Proposed General and Specific Prohibitions' (Report, November 2024).

[77] An alternative to including the requirement of 'unreasonableness' is being contemplated, namely to instead include a requirement that the conduct not be 'reasonably necessary to protect the business' legitimate interests'.

[78] Australian Treasury, 'Unfair Trading Practices: Consultation on the Design of Proposed General and Specific Prohibitions' (Report, November 2024) p. 8.

[79] For example, the AFP, in liaison with INTERPOL, is actively working to deter and prevent scam operations in 'boiler rooms' focused on South East Asia and Eastern Europe (AFP, 'Operation Firestorm to Target Cyber Scammers Cheating Australians' (Media Release, 28 August 2024)).

[80] Statistica, 'Artificial Intelligence - Worldwide' (Webpage, July 2024).

[81] For example, in March 2024, the US Securities Exchange Commission settled charges against two investment advisors (Delphia (USA) Inc and Global Predictions Inc) for making false or misleading statements about their purported use of AI (SEC, 'SEC Charges Two Investment Advisers with Making False and Misleading Statements About Their Use of Artificial Intelligence' (Media Release, 18 March 2024)). In October 2023, Pixelup was found in the UK to have breached the Advertising Standards Authority's Code of Conduct for misleading consumers in its Instagram post (ASA, 'ASA Ruling on Codeway Dijital Hizmetler Anonim Sirketi t/a Codeway' (Media Release, 18 October 2023)).

[82] Consumers International, 'Connection and Protection in the Digital Age: The Internet of Things and Challenges for Consumer' (Report, April 2016) p. 33.

[83] ACL s 2 (definition of 'goods' (e)).

[84] ACCC, 'iPhone and iPad Misrepresentations Cost Apple Inc $9 Million in Penalties' (Media Release, 19 June 2018). In that case, Apple was fined $9 million for making false or misleading representations to customers with faulty iPhones and iPads about their rights under the consumer guarantees. The ACCC took action against Apple following an investigation into complaints relating to 'error 53' which disabled some iPhones and iPads after owners downloaded a software update. The Federal Court found that the ios8 and ios9 software updates supplied to consumers were subject to the consumer guarantees, including that the 'goods' be of acceptable quality and reasonably fit for purpose.

[85] ACL s 274.

[86] ACL ss 122-128.

[87] Jeffrey Dastin, 'Insight - Amazon scraps secret AI recruiting tool that showed bias against women' (News Article, Reuters, 11 October 2018).

[88] Parliament of Australia, 'The Future of Work' (Report, Standing Committee on Employment, Education and Training, January 2025).

[89] Ibid.

[90] Parliament of Victoria 'Inquiry into Workplace Surveillance' (Report, Economy and Infrastructure Committee, May 2025).

[91] Jonathan Keane, 'Deliveroo rating algorithm was unfair to riders, Italian court rules' (News Article, Forbes, 5 January 2021).

[92] Australian eSafety Commissioner, 'How eSafety Can Help' (Webpage, accessed June 2025).

[93] Supreme Court of New South Wales, 'Supreme Court Practice Note SC Gen 23: Use of Generative Artificial Intelligence (AI)' (28 January 2025).

[94] Ibid [7].

[95] Ibid [16].

[96] Ibid [18].

[97] A similar scenario was the subject of *Dayal* [2024] FedCFamC2F 1166. In 2024, a Victorian lawyer (Mr Dayal) tendered a list of authorities to the Federal Circuit and Family Court of Australia in a family law case. Neither the Judge nor Her Honours' associates were able to locate the authorities listed. Mr Dayal admitted to preparing the list of authorities using an AI research tool and acknowledged that he did not verify the accuracy of the results. Mr Dayal apologised for his conduct, stated that he 'did not fully understand how the research tool worked', and acknowledged 'the need to verify AI assisted research … for accuracy and integrity'.
Although the Judge accepted Mr Dayal's apology and found that such conduct was unlikely to be repeated, the Judge still found it necessary to refer Mr Dayal's conduct to the Victorian Legal Services Board. In making that referral, the Judge noted that the Supreme Court of Victoria and the County Court of Victoria have published guidelines that emphasise the need for lawyers to 'exercise judgment and professional skill' in reviewing the work produced by AI.

[98] [2024] VCC 182.

[99] Australian Productivity Commission, 'Making the Most of the AI Opportunity - Research Paper 2: The Challenges of Regulating AI' (Report, January 2024) p. 5.

[100] Tim Ayres, 'Keynote to the AFR AI Summit' (Speech, 3 June 2025).

[101] *Bartz v. Anthropic PBC*, 3:24-cv-05417, (N.D. Cal.).

102 Australian Productivity Commission, 'Making the Most of the AI Opportunity - Research Paper 2: The Challenges of Regulating AI' (Report, January 2024) p. 1. We echo the observations by the Productivity Commission: '*As with any new technology, some consequences of AI use will only become apparent as the technology develops further and complementary technologies progress and are taken up. With general purpose technologies in particular, regulation based on 'predicted uses' or 'speculated harms' is likely to be overly broad and harm productivity. Many potential harms have been encountered with past technologies and adequately dealt with by existing regulatory frameworks in areas such as consumer protection, privacy, anti-discrimination, negligence and sector-specific and profession-specific requirements. AI is no different.*'

103 Australian Government, 'The Australian Government Guide to Regulation' (Report, March 2014) p. 2.

104 Australian Productivity Commission, 'Best Practice Regulation Handbook', (Report, August 2007).

105 Australian Productivity Commission, 'Making the Most of the AI Opportunity - Research Paper 2: The Challenges of Regulating AI' (Report, January 2024) p. 9.

106 Ibid p. 11.

107 ASIC, 'Beware the Gap: Governance Arrangements in the Face of AI Innovation' (Report, October 2024), which examined the ways Australian financial services and credit licensees are implementing AI where it impacts consumers and found there is the potential for a governance gap.

108 For example, a key pillar of the Singapore government's National AI Strategy is AI talent and education: to further help Singaporeans understand the fundamentals and applications of AI, be it in their workplace or daily lives, SkillsFuture Singapore has partnered with major technology partners, to offer a SkillsFuture for Digital Workplace program with relevant AI content, which is subsidised by the Singapore government, and the Singapore government has funded free AI literacy courses for the general public. Smart Nation Singapore, 'National Artificial Intelligence Strategy - Advancing our Smart Nation Journey' (Report, November 2019) and AI Singapore 'AI for Everyone' (Webpage, accessed June 2025).

109 Australian Productivity Commission, 'Support Safe Data Access and Handling Through an Outcomes-based Approach to Privacy' (Webpage, accessed June 2025).

110 This obligation was introduced under the *Privacy and Other Legislation Amendment Act 2024* (Cth) (Tranche 1 of the Privacy Act reforms) and came into effect on 11 December 2024.

111 This provision was introduced as part of Tranche 1 of the Privacy Act reforms and came into effect 10 June 2025, and is commonly referred to as the statutory tort for invasion of privacy. There is also the possibility of a similar action being brought at common law, as seen recently at the County Court level in the State of Victoria, in *Waller v Barrett* [2024] VCC 962. The elements of this tort for serious invasion of privacy have not been confirmed by a higher court, and remain unclear. The possibility of a common law tort for serious invasion of privacy being recognised has remained open since the High Court's decision in *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199.

112 The Code was introduced as part of Tranche 1 of the Privacy Act reforms. It must be developed and registered by 10 December 2026.

113 Parliament of Australia, 'The Future of Work' (Report, Standing Committee on Employment, Education and Training, January 2025).

114 *Reckitt and Colman Products Ltd v Borden Inc* (1990) 17 IPR 1, 8.

115 *International Covenant on Civil and Political Rights* (entered into force 23 March 1976) art 19.

116 *Online Safety Act 2021* (Cth) s 5.

117 Robert Mueller, 'Report on the Investigation into Russian Interference in the 2016 Presidential Election' (Report, Volume 1, March 2019) pp 4-5.

118 Second Reading Speech, National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017.

119 Australian Security Intelligence Organisation, 'Director-General's Annual Threat Assessment 2025' (Speech, 19 February 2025).

120 Sections 92.6 and 15.2 of the Criminal Code.

121 [2024] VCC 182, [4].

122 *LibertyWorks Inc v Commonwealth of Australia* (2021) 274 CLR 1, 14 [11] per Kiefel CJ, Keane and Gleeson JJ.

123 Parliament of Australia, 'Review of the Foreign Influence Transparency Scheme Act 2018' (Report, Parliamentary Joint Committee on Intelligence and Security, March 2024).

124 Section 61A of the *Foreign Influence Transparency Scheme Act 2018* (Cth) and section 14.1 of the Criminal Code.

125 Rule 6(l) of the *Foreign Influence Transparency Scheme Rules 2018* (Cth).

Ashurst

This publication is not intended to be a comprehensive review of all developments in the law and practice, or to cover all aspects of those referred to. Readers should take legal advice before applying the information contained in this publication to specific issues or transactions. For more information please contact us at aus.marketing@ashurst.com.

Ashurst Australia (ABN 75 304 286 095) is a general partnership constituted under the laws of the Australian Capital Territory and is part of the Ashurst Group. Further details about Ashurst can be found at www.ashurst.com.

ashurst.com

Design Ref: R014281 Aug 25