

Legal 500

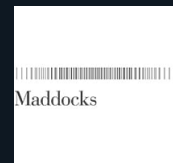
Country Comparative Guides 2026

Australia

Artificial Intelligence

Contributor

Maddocks



Sonia Sharma

Partner | sonia.sharma@maddocks.com.au

Ooma Khurana

Partner | ooma.khurana@maddocks.com.au

Greg Palumbo

Partner | greg.palumbo@maddocks.com.au

Nick Topfer

Special Counsel | nick.topfer@maddocks.com.au

Avi Kohli

Senior Associate | avi.kohli@maddocks.com.au

Shivani Thirayan

Senior Associate | shivani.thirayan@maddocks.com.au

This country-specific Q&A provides an overview of artificial intelligence laws and regulations applicable in Australia.

For a full list of jurisdictional Q&As visit legal500.com/guides

Australia: Artificial Intelligence

1. What is the legal definition of "artificial intelligence" in your jurisdiction, if any? If no definition exists, how do regulators or courts typically describe artificial intelligence?

Australia has no single statutory or judicial definition of "artificial intelligence".

Australian regulators and courts commonly distinguish between 'machine learning' or LLMs and AI, and often adopt or reference the Organisation for Economic Co-operation and Development's (OECD's) definition, which describes 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."

Australia's national Privacy Regulator, the Office of the Australian Information Commissioner, notes that, "while there is no single agreed definition of artificial intelligence (AI), as a general term it refers to the ability of machines to perform tasks which normally require human intelligence."

Although the Australian courts have engaged with AI in specific contexts, these cases have not yet defined AI as a legal concept and there is currently no judicially agreed definition of artificial intelligence.

2. Has your country developed a national strategy for artificial intelligence? If yes, what progress has been made in its implementation? Are there plans for updates or revisions?

The Commonwealth Government released a National AI Plan on 2 December 2025 that sets out the steps the Australian Government will take to "support Australia to build an AI-enabled economy that is more competitive, productive and resilient".

The National AI Plan has three objectives: capturing economic opportunities, sharing benefits across society, and keeping Australians safe through robust legal and

regulatory frameworks.

Key implementation measures from the National AI Plan include:

- the establishment of an Australian AI Safety Institute (AISI),
- a Chief AI Officer in every Commonwealth agency,
- launching an 'AI Accelerator' funding round of the Cooperative Research Centres (CRC) program;
- supporting the AI Adopt program, which helps small and medium-sized businesses implement AI; and
- expanding the National AI Centre.

The Australian government has implemented several of its identified key measures since the National AI Plan was released, including by allocating \$70 million in grant funding to the AI Accelerator to help develop local AI capability and \$30 million to the establishment of AISI. In May 2026, Australia also signed agreements with partner AISI institutes in the UK and Canada, giving AISI access to shared testing methods, shared expertise, and shared intelligence on the risks of advanced AI systems.

While there are no published plans to formally revise the National AI Plan, the establishment of the Office of AI in July 2026 to develop and legislate the mandatory Australian Standards for AI represents a significant new implementation measure that is likely to materially affect Australia's AI governance framework. See Questions 3 and 16 for further details.

3. Has your jurisdiction adopted any AI-specific laws, regulations, voluntary standards, or ethical guidelines? If so, please provide a brief overview. If not, which existing laws could be/applied to artificial intelligence and the use of artificial intelligence, what are the main interpretive challenges, and are there any pending artificial intelligence legislative initiatives?

Unlike the EU, Australia has not adopted a dedicated legislative framework for the regulation of AI systems or products. Instead, Australia seeks to adopt a technology-neutral approach to AI regulation, relying on existing laws

(including privacy, consumer, copyright, discrimination and sector-specific regulation), supplemented by targeted legislative reforms and regulatory guidance to address the use of AI in relation to identified high-risk use cases.

To date, examples of targeted legislative reform include:

- amendments to the *Privacy Act 1988* (Cth) to introduce new automated decision making transparency obligations (see Question 4. below).
- amendments to the *Work Health and Safety Act 2011* (NSW) to introduce a "Digital Work System Duty" on persons conducting a business or undertaking (PCBUs) to ensure that the health and safety of workers is not put at risk by the allocation of work through a digital work system (see Question 12 below).
- the introduction of the Online Safety (Basic Online Safety Expectations) Amendment Determination 2024 to impose obligations on service providers to consider user safety in the design and implementation of services and products that have generative AI capabilities (see Question 5 below).

Australia has focused heavily on producing guidance and governance measures to assist businesses and organisations with the adoption and deployment of AI systems, including *Guidance for AI Adoption* (October 2025), published by the National AI Centre (NAIC), which streamlined the 10 Voluntary AI Safety Standards (2024) and Australia's 8 AI Ethics Principles (2019) into six essential AI practices to support safe and responsible use of artificial intelligence.

In July 2026, the Commonwealth Government announced plans to legislate AI standards for data centres, reiterated its intention to ensure that creative works are protected by copyright, and announced the establishment of a new Office of AI.

Key takeaways from the announcement are as follows:

- **Regulation of Data Centres:** The standards will impose specific requirements for data centres, including requirements to be as water efficient as possible, reduce power when required to strengthen the grid, pay connection costs to ensure energy costs are not impacted, and be legally obliged to underwrite their own new power supply, and also include rules for where data centres can be built.
- **Strengthen copyright and artist protections:**

The Government reiterated its intentions to ensure that:

- artists, journalists, musicians and writers retain ownership and control of their work;
 - companies are not permitted to use Australian content for training of AI models without the artist's consent; and
 - artists retain control over pricing and licensing of their creative works.
- **Creation of a new Office of AI:** The Office of AI will work closely with the Minister for Industry and Innovation, and the Assistant Minister for Science, Technology and the Digital Economy, to oversee the development of the Australian Standards for AI, accelerate the national implementation of the standards and facilitate a whole-of-government approach.

4. Are there legal requirements for artificial intelligence transparency, explainability, or audits? Are there obligations to disclose the use of artificial intelligence to customers/clients?

From 10 December 2026, under new Australian Privacy Principles (APP) 1.7 to 1.9, entities covered by the Privacy Act (APP Entities) must disclose in their APP 1 Privacy Policy the use of automated decision making (ADM), where they have used computer programs (including artificial intelligence) and personal information to make a decision that could be reasonably expected to significantly affect the rights or interests of an individual.

Under APP 1.8, APP entities must update their privacy policies to disclose:

- the kinds of personal information used in the operation of computer programs;
- the kinds of decisions made solely by the operation of computer programs; and
- the kinds of decisions for which a thing, that is substantially and directly related to making the decision, is done by the operation of such computer programs.

In addition to the mandatory ADM obligations set out above, APP entities also have notification obligations under the Privacy Act to:

- have a clearly expressed, up-to-date and publicly accessible APP Privacy Policy about

how the entity manages personal information (APP 1);

- take reasonable steps to make individuals aware of certain mandatory matters before, or at the time it collects personal information, such as the fact and circumstance of collection and the purpose of collection (APP 5). Practically, APP 5 is discharged through bespoke and specific collection notices provided at the time of collection (such as a collection notice provided with a registration form).

In relation to both notification obligations, guidance from the Australian Privacy Regulator, the Office of the Australian Information Commissioner (OAIC), sets out expectations regarding the level of granularity and specificity of information to be provided, which will vary depending on the nature, context and sensitivity of the personal information being collected. Where artificial intelligence is used to collect, use or otherwise process personal information, including for the development, testing or training of artificial intelligence systems, in addition to mandatory ADM disclosure requirements, APP entities should have regard to APP 1 and APP 5 and their associated transparency requirements more generally. Consistent with guidance from the Privacy Regulator, APP Entities should also update their APP 1 privacy policies and APP 5 notifications with clear and transparent information about their use of AI, including ensuring that any public facing AI tools (such as chatbots) are clearly identified as such to users.

Regarding audits and explainability, there are currently no specific legal requirements for AI audits under Australian law. However, existing technology-neutral obligations will apply to AI systems that handle personal information. For example, APP 11 requires APP entities to take reasonable steps to implement organisational and technical measures to protect personal information. This includes maintaining appropriate logs (such as AI incident logs) and putting in place measures to monitor how the AI system performs. Regulatory guidance from the OAIC also encourages organisations to keep records of, and to test and monitor, any AI systems used in connection with personal information. In addition, APP 1 requires an APP Entity to take reasonable steps to comply with the APPs. Consistent with guidance from the Privacy Regulator, organisations considering the use of AI products should consider taking a 'privacy by design' approach, which includes conducting a Privacy Impact Assessment and establishing policies and procedures for the use of AI systems to facilitate transparency and ensure good privacy governance. Recent enforcement action in

Australia indicates that, for an AI deployment, "reasonable steps" for the purpose of APP 1 and 11 would be closely examined, including in respect of transparency, explainability and audits.

While not mandated, 'Share essential information' is also one of the 6 Essential AI Practices, which encourages organisations to inform users and stakeholders when and how they are interacting with AI. The Privacy Regulator also strongly encourages businesses and organisations to provide clear and transparent information about their use of AI generally in their privacy policies.

5. Are there legal requirements or best practice expectations for human oversight and human-in-the-loop in artificial intelligence systems?

There are no legislative requirements in Australia that expressly require human oversight and human-in-the-loop in AI systems. However, recent guidance in the form of strongly worded warning letters calling for urgent attention on managing AI risks from Australian regulators such as APRA, ASIC and the ACSC reflects a consistent regulatory expectation that organisations deploying AI implement robust governance, accountability and risk management frameworks.

Common themes include board and senior management responsibility for AI-related risks, maintaining sufficient AI literacy to support effective oversight, implementing governance and monitoring processes proportionate to the relevant use case, ensuring clear accountability for AI outcomes, and maintaining meaningful human oversight, or a "human-in-the-loop" approach, for high-risk, consequential or customer-facing decisions. Taken together, this guidance indicates an increasing expectation that organisations adopt structured governance arrangements for the safe, responsible and sustainable use of AI throughout its lifecycle, supported by appropriate policies, controls, documentation, training and ongoing oversight. APRA and ASIC both have enforcement powers and have demonstrated an increased willingness to hold Boards and directors to account where governance and risk management failures occur in respect of cyber security issues more generally.

In addition to the recent regulatory letters, the following guidance and determination have also been released:

- the Guidance for AI Adoption (October 2025) published by National AI Centre (NAIC) sets out best practice expectations for responsible AI use and "Maintain human control" is one of the six essential AI practices. NAIC

recommends that organisations should have appropriate and meaningful human oversight of any AI systems in use.

- Similar expectations are also reflected in Australia's Online Safety framework for providers of generative AI services. The Online Safety (Basic Online Safety Expectations) Amendment Determination 2024 (BOSE Determination) also imposes an obligation on certain providers that use or enable generative AI capabilities to "take reasonable steps to consider user safety and incorporate safety measures in the design, implementation and maintenance of those generative AI capabilities". Examples of reasonable steps include having appropriately resourced trust and safety teams to "ensure that appropriate safety interventions are in place, that interventions are working effectively, and that safety issues are responded to as a priority."

In light of the strong regulatory focus on AI risk management and warnings issued in regulatory guidance, a failure to implement appropriate oversight, governance and accountability measures may increase regulatory enforcement risk, including regulatory investigations, remediation requirements, infringement notices, licence-related consequences and, in appropriate circumstances, enforcement action against the organisation and its responsible officers.

6. Are there specific legal or regulatory requirements addressing algorithmic bias, discrimination, or fairness in AI systems (including gender bias)?

Australia has no AI-specific anti-discrimination legislation addressing algorithmic bias. However, existing federal and state anti-discrimination laws (including the Fair Work Act 2009 (Cth), Racial Discrimination Act 1975 (Cth), Sex Discrimination Act 1984 (Cth), Disability Discrimination Act 1992 (Cth) and Age Discrimination Act 2004 (Cth)) apply regardless of whether a decision is made by a human or an AI system.

In the Australian Human Rights Commission's Technical Paper: Addressing Algorithmic Bias (2020) the AHRC established that algorithmic bias can constitute unlawful direct or indirect discrimination under these statutes, and recommended rigorous design, testing and monitoring to avoid it.

A number of Australian, state and territory governments have developed and adopted published guidance or

policies which incorporate principles relating to the ethical use of AI and with a stated intention to ensure use of AI complies with legal protections for human rights and basic principles of fairness.

The Australian Consumer Law may also capture unfair algorithmic outputs, with the Australian Competition and Consumer Commission confirming that entities cannot avoid liability for misleading or deceptive conduct by attributing it to an automated system.

7. What legal frameworks apply to AI-related harm and defective artificial intelligence systems? Who can be held liable (developer, deployer, victim of the damage, others), how is liability allocated, and what burden of proof applies to victims?

While there is no AI-specific liability statute in Australia, the Australian Government's 2025 Review of AI and the Australian Consumer Law (Review) concluded that the existing technology-neutral protections under the Australian Consumer Law (ACL), which is Schedule 2 to the Competition and Consumer Act 2010 (Cth), are generally capable of addressing AI-related consumer law risks. This means that the established principles under the ACL regarding misleading or deceptive conduct, false representations, consumer guarantees and product safety provisions would apply to AI-enabled goods and services.

Under the ACL, manufacturers may be held liable in respect of personal injury and property damage caused by a "safety defect" in their product. Goods have a "safety defect" if they are not as safe as a consumer would generally expect. The ACL defines the scope of a "manufacturer" broadly to include persons who produce goods (including computer software) as well as importers and persons who permit their brand to be applied to goods. This broad definition could encompass AI developers, deployers, suppliers or distributors depending on the circumstances.

The burden of proof lies with the claimant seeking a remedy. The claimant must establish, on the balance of probabilities, that the claimed loss was caused by a failure of a consumer guarantee or malfunction of a good. Claimants can take legal action against manufacturers or lodge a complaint with the regulator.

Under the consumer guarantees regime in the ACL, customers of defective AI products may also have recourse against a supplier (including retailers) that is not

a manufacturer. The consumer guarantees regime provides for non-excludable warranties in respect of goods and services supplied to consumers – for example, products and services must be of acceptable quality.

8. What cybersecurity obligations apply to AI systems?

There is no single cybersecurity legislation or framework that applies exclusively to AI systems.

However, there are a number of cybersecurity-related policies and legislative frameworks that apply to technology systems generally, including AI systems and systems which use or host AI models.

Legislative frameworks include:

- **The Cyber Security Act 2024 (Cth)** – Australia's first standalone cyber security legislation. This Act includes a framework for mandatory security standards for certain smart devices and mandatory ransomware payment reporting obligations. To the extent AI functionality is incorporated into products captured by the legislation, those products may also be subject to these requirements.
- **The Security of Critical Infrastructure Act 2018 (Cth)** – imposes cyber security incident reporting obligations and, for responsible entities of critical infrastructure assets, critical infrastructure risk management program obligations. Where AI systems form part of the operation of a critical infrastructure asset, risks associated with those systems may need to be addressed within the entity's broader risk management framework.
- **The Privacy Act 1988 (Cth)** – requires APP entities to take reasonable steps to protect personal information from misuse, interference and loss (APP 11), which applies to data processed by AI systems, including personal information used as AI inputs, training data and outputs.

At the State and Territory governmental level, AI systems are also generally regulated through existing privacy, information management and public sector governance legislation rather than AI-specific statutes. Key examples include various State and Territory privacy acts that are similar to the Privacy Act 1988 (Cth). However:

- many State-owned utilities and infrastructure operators may also be subject to the Security

of Critical Infrastructure Act 2018 (Cth) where they operate assets falling within the Commonwealth regime; and

- certain provisions of the Cyber Security Act 2024 (Cth), including the smart-device security framework in Part 2, may apply to entities involved in the manufacture, importation or supply of relevant connectable products irrespective of government ownership.

Government entities may also be subject to separate policy requirements relevant to cyber security. Government entities may 'flow down' obligations to comply with these policy requirements when purchasing relevant goods and services from private industry. These include obligations not to use certain banned AI systems, and other relevant obligations relating to location of hosting for certain types of data, encryption and cybersecurity risk assessments.

9. Is the use of artificial intelligence insured and/or insurable in your jurisdiction, including with cyber policies? Are there market trends, or limitations?

Yes. While dedicated AI insurance products are still emerging, AI-related risks are often already covered under existing insurance policies through so-called "silent AI" coverage, where policies respond to AI-related losses without expressly referring to AI.

Insurance in Australia is generally technology-neutral, and AI-specific claims data remains relatively limited. As a result, insurers typically assess AI-related losses under traditional insurance lines unless coverage is expressly excluded. Depending on the circumstances, AI-related risks may be covered under professional indemnity, directors' and officers' liability, product liability, cyber, employment practices liability, and property damage/business interruption policies.

Cyber insurance is currently one of the primary forms of cover for AI-related risks. Traditional cyber policies generally respond to losses arising from privacy breaches, security failures, incident response and recovery costs, data restoration, media liability, and business interruption. Insurers are increasingly incorporating AI-specific underwriting questions and, in some cases, issuing AI-related endorsements as they seek to better understand and price AI risk.

However, coverage may be limited by exclusions, sub-limits, or other policy restrictions. Common areas of concern include intellectual property infringement,

discriminatory or biased AI outputs, performance or warranty-related claims, regulatory investigations and penalties, and systemic or catastrophic cyber events.

Organisations adopting AI should carefully review their existing insurance arrangements to determine whether AI-related losses are covered and whether any exclusions, conditions, or coverage gaps may apply. In some cases, organisations may need to seek bespoke endorsements or specialised cyber coverage to address AI-specific risks.

10. Can artificial intelligence be named as an inventor in a patent application filed in your jurisdiction? If not, what is the current legal position?

Artificial intelligence cannot be named as an inventor for a patent application filed in Australia. The current legal position is that an inventor must be a natural person (which was established by an enlarged bench of the Full Court of the Federal Court of Australia in *Commissioner of Patents (Cth) v Thaler* [2022] FCAFC 62, and effectively endorsed by the High Court of Australia by its refusal to grant Mr Thaler special leave to appeal the decision).

11. Do images or works generated by and/or with artificial intelligence benefit from copyright protection in your jurisdiction? If so, who is the authorship attributed to, and under what conditions?

In Australia, AI-generated work without any human contribution is unlikely to attract copyright protection. Under the Copyright Act 1968 (Cth), copyright protection is granted to original literary, dramatic, musical and artistic works that originate from an "author" and are expressed in material form.

While 'author' is not defined in the Copyright Act 1968 (Cth), Australian courts have consistently interpreted "author" as requiring human authorship. In *Telstra Corporation Ltd v Phone Directories Co Pty Ltd* [2010] FCAFC 149, the Full Federal Court held that works generated by automated processes without sufficient human 'intellectual effort' did not attract copyright protection.

While it's possible that where a human exercises sufficient creative control, for example through detailed prompting, curation, editing and selection, the human authorship requirement may be satisfied, with copyright

protection vesting in that individual, this position remains untested by Australian courts in the generative AI context.

In July 2026, the Australian Government also reiterated its intention to strengthen copyright protections for artists, writers and musicians (for more about this see Question 3).

12. What are the main issues to consider when using artificial intelligence systems in the workplace? Have any new regulations, or guidelines, been introduced regarding AI-driven hiring, performance assessment, or employee monitoring?

The main workplace issues to consider when using AI systems include:

- bias and discrimination in AI-driven hiring and performance management;
- work health and safety risks, including psychosocial hazards from AI-driven role uncertainty and over-reliance on AI in decision-making, including in rostering and work allocation;
- the use of AI in employee performance monitoring and surveillance;
- employee data privacy obligations;
- whether consultation obligations apply when introducing AI that impacts roles; and
- the development of workplace policies and training on appropriate AI, including risks of unauthorised use of AI tools.

Australia's existing workplace and discrimination laws are technology-neutral and employers remain responsible and liable for decisions made or materially influenced by AI, including recruitment, promotion, performance management or dismissal decisions. Employers must also assess and manage AI related risks in order to comply with their general WHS duty of care.

NSW is currently the first Australian State to specifically regulate AI risks in the workplace. Under recent amendments to its WHS laws (yet to commence), a person conducting a business or undertaking must:

- ensure, so far as is reasonably practicable, that a worker's health and safety is not put at risk from the use of a 'digital work system' (which includes AI), including in work allocation; and
- consider whether its use of digital work systems creates or results in risks concerning

excessive or unreasonable monitoring or surveillance, performance metrics, workloads, or unlawful discriminatory practices or decision making.

The amendments also empower union officials to access and inspect a PCBU's digital work systems relevant to a suspected breach of WHS obligations.

13. What are the main privacy/data protection issues arising from artificial intelligence development and use (including training data)? Have data protection authorities issued guidelines or rulings on artificial intelligence, and what are the key takeaways?

The main privacy and data protection issues arising from AI development and use in Australia relate to the collection, use, disclosure and retention of personal information, particularly where AI systems are trained on large datasets containing personal information. Key risks include:

- Training data collection: AI models may be trained on personal information scraped from websites, social media or other sources without individuals' knowledge or consent, raising issues under the Privacy Act and Australian Privacy Principles (APPs).
- Purpose limitation and secondary use: Using personal information to train an AI model may go beyond the purpose for which the information was originally collected, potentially breaching APP 6 (which requires entities to only use or disclose the information for the primary purpose for which it was collected, unless an exception applies).
- Transparency and notice: Organisations may fail to adequately inform individuals that their personal information is being used in AI systems or for model training.
- Accuracy and hallucinations: AI systems may generate incorrect, inferred or fabricated information about individuals. The OAIC considers such information to be "personal information" where it relates to an identifiable individual.
- Security and cross-border disclosures: Inputting personal information into third party AI tools may constitute a disclosure, often involving overseas processing and associated security risks. Terms of use for various AI tools often explicitly state that information input into

the AI tool may be accessed by the company that owns that tool.

- Automated decision-making and profiling: AI systems can infer sensitive characteristics or make decisions affecting individuals, raising concerns about fairness, explainability and accountability.

The main data protection authority in Australia, the Office of the Australian Information Commissioner (OAIC) has issued substantial guidance on these issues. The OAIC's central position is that there is no "AI exemption" from the Privacy Act; existing APP obligations apply to AI inputs, training data and outputs.

Key takeaways from the OAIC guidance include:

- Privacy obligations apply to both AI inputs and outputs containing personal information.
- Organisations should conduct privacy impact assessments, undertake vendor due diligence and implement strong governance before deploying AI systems.
- Privacy policies and collection notices should clearly explain AI-related uses of personal information.
- Personal information, particularly sensitive information, should generally not be entered into publicly available generative AI tools unless privacy risks have been appropriately managed.
- AI-generated or inferred information about identifiable individuals must be handled in accordance with the APPs.

Overall, Australian regulators are taking the view that existing privacy laws already apply to AI, and organisations must adopt a "privacy by design" approach when developing and deploying AI systems.

14. How is data scraping regulated in your jurisdiction from an IP, privacy and competition perspective? Are there recent precedents addressing the legality of data scraping for training of artificial intelligence systems?

Data scraping activities present multiple legal and regulatory risks.

The Privacy Act imposes obligations on entities governed by the Act who 'data scrape' personal information. Under Australian Privacy Principle 3, businesses may generally only collect personal information directly from the individual unless it is unreasonable or impracticable to do

so. Consent is also required where the collection of personal information pertains to sensitive information. There are very limited exceptions to these requirements.

In recent years, the Office of the Australian Information Commissioner (OAIC) has also warned that web scraping raises "significant privacy concerns", particularly where personal information is scraped without the knowledge of the data subject and against their expectations.

The OAIC has recently taken action against multiple businesses in relation to data scraping activities:

- **Clearview AI.** Following enforcement action taken by the OAIC, the Administrative Appeals Tribunal (AAT) found that Clearview AI had unlawfully collected personal information via data scraping. Clearview AI had been scraping social media platforms to collect images of individuals for the purposes of building a facial recognition database for use by law enforcement agencies. Notably, the Tribunal held that Clearview AI had failed to obtain individuals' consent before collecting their sensitive biometric information.
- **DG Institute and Property Lovers.** The OAIC took enforcement action against DG Institute and Property Lovers in relation to the scraping of court lists, death and funeral notices and other publicly available data to generate leads lists. The OAIC determined that DG Institute and Property Lovers had collected personal information via "unfair" means, having regard to the purpose of the leads list (i.e. marketing activities) and the vulnerability of the affected individuals. The OAIC also determined that the entities had failed to notify the individuals of the collection, failed to maintain the accuracy of the information and failed to maintain an adequate privacy policy.

In some cases, data scraping may also infringe copyright in the scraped material. In October 2025, the Attorney-General confirmed that Australia will not introduce a text and data mining exception under the Copyright Act 1968 (Cth) that would allow AI companies to use Australian copyrighted materials for training purposes without permission of or compensation to the creator, citing its rationale behind this was to provide certainty to creators and to ensure that they are fairly compensated for providing their copyrighted material for AI training. This position was reinforced in a speech by the Prime Minister in July 2026, despite pressure from leading global AI developers, in which he stated that Australia's laws will make clear that creators must retain ownership and

control of their work.

15. To what extent is the prohibition of data scraping in the terms of use of a website enforceable?

Platform or website terms of use often prohibit data scraping. Whether and how that prohibition can be enforced is a nuanced question that turns on the parties, their contractual relationship (or lack thereof), the nature of the data, and the purpose of the data scraping. If the party doing the scraping has entered into a service agreement prohibiting such activity, enforcement is usually quite straightforward.

Although this question has been tested in the courts of other jurisdictions (including Europe and the United States), there is no definitive appellate authority squarely addressing the enforceability of website anti-scraping clauses. The issue was touched upon in the Clearview AI AAT Determination (see Question 14 above), however the Tribunal noted that it was not in a position to judge whether the interactions between Clearview's web-crawler and [LinkedIn and Twitter terms of service] amount to breaches of conditions of access.

Generally, Australian courts enforce properly incorporated online contractual terms, particularly click-wrap agreements. Accordingly, the overall view is that an express prohibition on data scraping is likely to be enforceable where the scraper has agreed to the relevant terms, subject to ordinary contractual principles and any competing statutory considerations.

16. Does your country have a regulator or authority responsible for supervising the use and development of artificial intelligence? What are its powers and enforcement tools?

Australia does not (yet) have a unitary AI Regulator. Instead, oversight is distributed through the regulators that pre-existed the emergence of the technology. These regulators form a distributed enforcement model, applying developing statutory powers. The most significant regulators are:

- **Office of AI** – on 15 July 2026, the Office of AI was established in the Department of the Prime Minister and Cabinet. The Office will coordinate across Australian Government agencies to develop and legislate the new Australia artificial intelligence standard and unlock AI training in Australia. These

standards will include mandatory requirements for large AI data centres, including setting standards for energy and water, with strong copyright protections for Australian creators. For more information, see Question 3. At this stage, the Office of AI does not have enforcement powers.

- **Office of the Australian Information Commissioner (OAIC)** – The OAIC oversees the distinct privacy and freedom of information aspects of the technology. Its functions regularly it to apply the existing Australian Privacy Principles to AI-related issues, including data collection and algorithmic decision making. The OAIC can investigate complaints, conduct own-motion investigations, make determinations, seek enforceable undertakings and pursue civil penalty proceedings for serious or repeated privacy breaches. Recently, OAIC has been particularly active in relation to generative AI and biometric technologies (see our comment on the Clearview AI matter above).
- **Australian Competition and Consumer Commission (ACCC)** – The ACCC oversees AI from a consumer protection and competition law perspective, focusing in this context on unfair practices and market power exercised through the use of AI. It can compel information, accept enforceable undertakings, issue infringement notices and seek injunctions and penalties through the courts. Recently, the ACCC has scrutinised the use of algorithmic and AI-enabled systems by digital platforms through its Digital Platforms Inquiry work. It has indicated that existing competition and consumer protection laws apply equally to AI-enabled products and services.
- **Australian Securities and Investments Commission (ASIC)** – ASIC supervises AI used in financial services under the Corporations Act and related legislation, including algorithmic trading. It can impose licence conditions, issue stop orders, commence civil or criminal proceedings, and take action against misleading conduct or inadequate governance. ASIC has already issued guidance that responsibility for decisions made in this context cannot be outsourced to algorithms.
- **eSafety Commissioner and Australian Communications and Media Authority (ACMA)** – may regulate certain AI-related online content, communications services, deepfakes, online safety risks and automated

communications. Their powers include content removal notices, infringement notices and enforcement action under online safety and communications legislation.

17. How widespread is the adoption of artificial intelligence in businesses in your jurisdiction, and which sectors are leading?

Artificial intelligence adoption in Australia is widespread conceptually but remains uneven in practice, with a clear gap between intent and mature implementation. According to the Australia Responsible AI Index 2025 final report (sponsored by the Australian Government) (Report), approximately 78% of organisations recognise and agree with principles supporting ethical AI use, indicating strong awareness and willingness to engage with AI technologies. However, this high level of endorsement is not matched by practical uptake, as:

- the average response indicated organisations were in a 'developing' stage, with momentum for the adoption of responsible AI building;
- only 23% of responding organisations are actively implementing responsible AI practices and growing their AI maturity; and
- only 12% of responding organisations are considered "leading" in terms of mature adoption, scaling use at pace and adopting best-in-class practices. An implementation, or "saying-doing", gap persists, where businesses are experimenting with or planning for AI but have not yet embedded robust governance frameworks or operationalised its use at scale.

In terms of sectors leading the way in implementation and maturity, the Report indicates the top industries are (1) Information Media & Telecoms, (2) Health, Education and Government and (3) Financial & Other Services.

18. How is artificial intelligence used in the legal sector, by lawyers and/or in-house counsels? Are AI-driven legal tools widely adopted, and what are the main regulatory concerns?

Artificial intelligence is used in the Australian legal sector by lawyers and in house counsel to automate routine, process driven work and enhance efficiency. A 2025 report by the University of Melbourne identified common uses of GenAI legal tools to include drafting document summaries and chronologies, contract analysis, due diligence, and generating insights, recommendations and

predictions. Law firms are adopting a mix of legal generative AI chatbots and tools, including inhouse built chatbots (for example, Microsoft Azure AI bots) and bespoke legal technology (for example, Harvey, Legora and Claude for Legal).

LexisNexis's 2025-26 Australian Legal AI Survey Report has identified wide adoption of AI-driven legal tools, with 69% of respondents using or planning to use generative AI for legal work, 90% feeling confident using AI and 45% using AI for legal research.

Key concerns include client confidentiality and data security, with practitioners warned not to input sensitive information into unsecured AI systems, as well as accuracy risks (including hallucinated outputs), bias, and misleading results. The Law Society of New South Wales emphasises that lawyers retain full responsibility for their advice, and must not rely on AI outputs without independent verification.

19. What are the 5 key challenges and the 5 key opportunities raised by artificial intelligence for lawyers in your jurisdiction?

The key challenges raised by AI for lawyers in Australia include:

- Regulatory uncertainty and fragmentation – In helping navigate AI related legal matters, lawyers, on behalf of their clients, must navigate evolving guidance from multiple regulators including the OAIC, ACCC, ASIC and eSafety Commissioner, while advising clients in an environment where legal obligations are still developing. The forthcoming mandatory Australian AI Standard, to be developed by the newly established Office of AI, will add a further layer of compliance obligations for lawyers and their clients to navigate.
- Privacy, data governance and AI training data – AI systems frequently raise complex questions regarding the collection, use and disclosure of personal information, particularly where personal information is used to train models or appears in AI outputs. The OAIC's guidance and the Clearview AI litigation demonstrate increasing regulatory scrutiny of AI data practices. Lawyers are increasingly required to advise on lawful data acquisition, cross-border data transfers, consent mechanisms and privacy compliance.
- Professional responsibility and legal practice risks – Law firms themselves face risks when

using generative AI. Issues include confidentiality, legal professional privilege, hallucinated authorities, inaccurate outputs and inadequate supervision of AI-generated work product. Lawyers remain responsible for the accuracy of legal advice regardless of whether AI tools were used in its preparation.

- Evidentiary reliability and litigation challenges – AI is creating novel evidentiary issues for courts and litigants. Lawyers are increasingly required to assess the provenance, reliability and authenticity of AI-generated content, including documents, images, audio and video. The growing prevalence of deepfakes, synthetic evidence and AI-assisted content generation raises difficult questions regarding admissibility, discovery, authenticity and expert evidence. At the same time, clients are increasingly seeking to rely on AI-generated outputs in decision-making and disputes, requiring lawyers to assess whether those outputs can withstand judicial scrutiny.
- Pressure on traditional legal service delivery and pricing models – AI has the potential to disrupt many of the economic assumptions on which legal practice has traditionally operated. Tasks that previously required significant lawyer time—such as first-pass contract review, due diligence, legal research, document summarisation and drafting—can increasingly be performed more efficiently using AI-assisted tools. This creates pressure on billable-hour models, fixed-fee pricing assumptions and traditional leverage structures within law firms. Clients are also becoming more sophisticated purchasers of legal services and may increasingly expect efficiency gains generated by AI to be reflected in pricing. For lawyers, the challenge is not merely adopting AI, but demonstrating value in a market where routine legal work is increasingly automated and strategic judgment, advocacy, negotiation and trusted advisory services become more important differentiators.

The key opportunities raised by AI for lawyers in Australia include:

- Transforming legal service delivery – AI can significantly improve productivity across legal research, document review, due diligence, contract analysis, discovery, drafting and knowledge management. This creates

opportunities to deliver legal services more efficiently, improve responsiveness and focus lawyer time on higher-value strategic work.

- Expansion of Technology practices – AI has created a major new advisory market. Clients increasingly require advice on AI procurement, governance, regulatory compliance, privacy, cybersecurity, intellectual property, liability allocation, responsible AI frameworks and sector-specific AI regulation. Many firms are developing dedicated AI practices in response, and lawyers are playing an increasingly important role in negotiating contractual protections around data use, model performance, intellectual property ownership, security, liability and regulatory compliance.
- Greater access to legal services – AI has the potential to reduce the cost of routine legal work and improve access to legal services for individuals and small businesses. Lawyers who effectively leverage AI may be able to offer services that were previously uneconomic to deliver.
- Building proprietary legal AI products and institutional knowledge assets – AI creates opportunities for law firms to move beyond traditional legal services and develop proprietary technology-enabled products. Firms may increasingly build internal models trained on their precedents, playbooks, negotiation positions, regulatory expertise and sector knowledge. Rather than AI simply increasing efficiency, it may enable firms to create scalable knowledge products, automated advisory tools and specialised legal intelligence platforms that complement traditional legal practice. Lawyers therefore have an opportunity to participate directly in the creation, training, governance and commercialisation of legal AI systems.
- Repositioning lawyers as strategic advisers – As routine work becomes increasingly automated, lawyers have an opportunity to focus on providing strategic judgment, negotiating and advocacy, stakeholder management, risk assessment and commercial decision-making. AI may therefore shift lawyers' roles from information providers to trusted advisers helping clients navigate complex legal, commercial and ethical questions.

20. Where do you see the most significant legal developments in artificial intelligence in your jurisdiction in the next 12 months? Are there any ongoing initiatives that could reshape AI governance?

Over the next 12 months, the most significant developments are likely to occur through the expansion of existing regulatory frameworks to AI, rather than through the enactment of a standalone Australian AI Act. A key exception is the development of a mandatory Australian AI Standard by the newly established Office of AI (see Questions 3 and 16), which is expected to introduce binding requirements covering AI governance, data centre infrastructure, and copyright protections for creators – representing the most significant structural change to Australia's AI regulatory landscape in the near term.

Key privacy reform and AI-related data governance changes are a particular area to watch. Further privacy reforms could materially affect AI development and deployment. For example:

- New Automated Decision Making Australian Privacy Principle – From 10 December 2026, entities that use a computer program to make, or do something substantially and directly related to making, a decision that could significantly affect an individual's rights or interests, and that uses personal information in doing so, will need to disclose this in their privacy policy and collection notices. This disclosure will need to clearly describe the kinds of personal information used, and the nature of the decision that will be affected. In AI terms, this will capture applications such as fraud risk scoring, eligibility triage, recruitment filtering and similar systems.
- Serious Invasion of Privacy Statutory Tort – The new statutory tort under the Privacy Act 1988 (Cth) creates a cause of action for serious invasion of privacy, including the misuse of information, with specific defences and remedies built into the regime. For AI developers and deployers, the tort may be triggered where systems are trained or operated using aggressively scraped datasets, biometric matching or other forms of information handling that look less like ordinary processing and more like intrusion or misuse.

Australia has also established the Australian AI Safety

Institute, which is intended to function as a technical and policy body whose role includes evaluating advanced AI systems, conducting safety assessments, supporting AI assurance and testing methodologies, and contributing to domestic and international AI safety initiatives. The Australian AI Safety Institute should play an important part in managing the AI sector (despite not being an enforcement regulator). However, whether its role will expand, contract or remain stable, and the practical influence it will have on AI in Australia, could determine the overall changes to the AI governance landscape in the near future.

Given Australia's land availability, technology vendors and property developers consider Australia as an important location for the construction of large-scale data centres and AI compute infrastructure. The rapid growth of these facilities is likely to become an increasingly important aspect of AI governance, as access to computing power is emerging as a strategic

prerequisite for the development, training and deployment of advanced AI systems.

This raises a range of legal and policy issues extending beyond the regulation of AI models themselves, including cyber security, critical infrastructure protection, foreign investment scrutiny, data localisation, sovereign capability, energy consumption and access to trusted computing environments for government and industry. In this regard, the Australian Government's National AI Plan places emphasis on strengthening Australia's domestic AI capability and supporting the infrastructure necessary to enable AI adoption and innovation. As investment in Australian data centre capacity accelerates, AI governance is likely to expand beyond questions of algorithmic accountability and data use to encompass the physical infrastructure on which AI systems are trained, hosted and operated, and the extent to which Australia can maintain sovereign control over strategically important AI capabilities.

Contributors

Sonia Sharma Partner	sonia.sharma@maddocks.com.au
Ooma Khurana Partner	ooma.khurana@maddocks.com.au
Greg Palumbo Partner	greg.palumbo@maddocks.com.au
Nick Topfer Special Counsel	nick.topfer@maddocks.com.au
Avi Kohli Senior Associate	avi.kohli@maddocks.com.au
Shivani Thirayan Senior Associate	shivani.thirayan@maddocks.com.au

