COUNTRY COMPARATIVE GUIDES 2023

The Legal 500 Country Comparative Guides

Australia

ARTIFICIAL INTELLIGENCE

Contributor

McCullough Robertson

Alex Hutchens

Partner | ahutchens@mccullough.com.au

Rebecca Lindhout

Senior Associate | rlindhout@mccullough.com.au

Sebastian Galetto

Lawyer | sgaletto@mccullough.com.au

Alex Komarowski

Lawyer | akomarowski@mccullough.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 are your countries legal definitions of “artificial intelligence”?

There is currently no single statutory definition of ‘artificial intelligence’ (**AI**) in Australia.

In various contexts, the Australian Government has endorsed the CSIRO’s working definition for AI, being:

‘a collection of interrelated technologies used to solve problems autonomously and perform tasks to achieve defined objectives without explicit guidance from a human being.’

although conversely, other definitions have been considered in the context of policy reform discussions.

The variety in definitions currently being considered across Australia demonstrates the inherent complexity in accurately articulating a technology with such broad characteristics.

2. Has your country developed a national strategy for artificial intelligence?

No national strategy has been implemented, although there have been several steps taken towards this.

After several interim steps by successive governments, on 1 June 2023, the Australian Government released an AI Discussion Paper, seeking submissions on the governance mechanisms available to ensure the safe development and use of AI in Australia, as well as feedback on the proposal to adopt a risk-based approach to governing AI (with the actual governance mechanism undecided). Submissions close 26 July 2023 and will inform Government regulatory and policy responses. In the next 12 months, it is likely we will see the Government’s response and potentially some draft legislation establishing an AI governance framework.

3. Has your country implemented rules or guidelines (including voluntary standards and ethical principles) on artificial intelligence? If so, please provide a brief overview of said rules or guidelines. If no rules on artificial intelligence are in force in your jurisdiction, please (i) provide a short overview of the existing laws that potentially could be applied to artificial intelligence and the use of artificial intelligence, (ii) briefly outline the main difficulties in interpreting such existing laws to suit the peculiarities of artificial intelligence, and (iii) summarize any draft laws, or legislative initiatives, on artificial intelligence.

Australia has approved the OECD’s recommendations on AI regulation and is a founding member of the Global Partnership on Artificial Intelligence, both of which aim to foster international collaboration on the responsible use and development of AI.

Further, the Australian Government has implemented a voluntary AI Ethics Framework, which is comprised of eight key ethical principles that are designed to ensure that AI systems developed in Australia are safe, secure and reliable. These principles largely mirror the OECD AI Principles. The Australian AI Ethics Framework is intended to complement other binding AI regulation when it is eventually implemented, but in the meantime there is minimal regulation of AI specifically in Australia.

While there are currently no specific Australian laws regulating the development and use of AI, a variety of existing legislation will be relevant to AI’s broader deployment in Australia, including to address its impact on market competition and consumer protection/product safety, intellectual property, data protection, privacy and cyber security, human rights and criminal law.

Each of these laws has its own nuance and specific requirements which will present challenges with their

 © 2023 Legalease Ltd

application to AI solutions. The overarching key difficulty with applying these existing laws to the use of AI is the fundamental lack of understanding of the way that an AI system arrives at its decisions. While there are calls for transparency and recording of the basis of decisions, the very nature of the algorithms is that their decision-making process cannot be perfectly reverse-engineered. More broadly, there is the usual regulatory risk of unintended consequences.

Specifically, the key challenges with applying existing laws to the use of AI will be as follows:

- competition law – with respect to the owners or suppliers of artificial intelligence technology, do the tools provide another avenue for abuse of dominance issues; and for users of the technologies, will access to these tools become a necessary means to compete, which will create issues with exclusivity arrangements and vertical integration.
- consumer protection law – there is a fundamental question about whether AI solutions will be 'goods' or 'services' under consumer protection laws, which has implications for what minimum standards the law will apply to the solutions (including in circumstances where high-level human thinking has previously been involved – e.g. in analysis and diagnosis); more broadly, there will also be difficult questions about liability when there is a supply chain involved (with only the manufacturers of 'goods' as opposed to 'services' having liability in some instances) and in determining the extent to which defences might be available, for instance in circumstances where there were not defects at the time of sale but through the AI's ongoing evolution later become defects without any subsequent intervention by any entity;
- intellectual property law – authorship is the key issue, as discussed below;
- data protection and privacy and cyber security – the fundamental tension between data privacy laws and the methods of obtaining training data for AI tools is already emerging in light of local caselaw (described below) and global enforcement activity, including in relation to the lawful basis of collection and processing of data, transparency around collection and usage limitation and data minimization principles;
- human rights – Australia's human rights regime relies on international treaties and a balancing of competing interests. Determining what appropriate use of AI looks like, and what controls are needed to challenge decision making in particular, will be ongoing challenges as AI decision making tools permeate increasingly large areas of public administration and corporate activity as it relates to its interaction with human individuals; and
- Criminal law – separately from the issue of potential criminal liability for an AI itself, or the supplier of an AI solution, the capabilities of generative AI to create authentic seeming "deep fake" content will potentially present evidentiary challenges.

4. Which rules apply to defective artificial intelligence systems, i.e. artificial intelligence systems that do not provide the safety that the public at large is entitled to expect?

In the absence of specific regulation relating to AI systems, liability for defects in AI systems will be governed by the terms of any applicable contract and also general law principles of contract, negligence and consumer law/product safety.

For the purchaser of an AI solution (or a product or service that incorporates AI technology), a failure of an AI solution to meet specifications, align with product definitions or perform expected functions will be actionable as breach of contract.

Separately, the supplier of an AI system may owe a duty of care to some or all of the public (its customers and then likely anyone who comes into contact with the product or the effects of its use), and if that sector of the public suffers loss or damage as a result of the AI's or AI provider's conduct, then it may be liable for those losses. If such a duty was able to be established, the determination of the relevant standard of care owed by the AI provider (that is, what precautions a reasonable person in the position of the AI provider would have taken) to its end users is likely to be an area of considerable uncertainty.

Further, to the extent that artificial intelligence systems are embedded within products sold to consumers (such as, by way of example, autonomous vehicles), then such products will be captured by the consumer guarantees contained in the Australian Consumer Law and the supplier and/or manufacturer may be liable for those breaches.

 © 2023 Legalease Ltd

Finally, the Australian Consumer Law also includes a product liability regime, as discussed in Question 5 below, which would apply to many AI solutions.

5. Please describe any civil and criminal liability rules that may apply in case of damages caused by artificial intelligence systems.

Product liability

In addition to the consumer guarantees, the Australian Consumer Law contains a product liability regime that may require manufacturers of AI systems to compensate consumers for injuries suffered due to defects in those systems. Consumers would need to establish that the AI system had a safety defect, that is, the AI system did not meet the safety level safety generally expected of it. Manufactures are strictly liable for actual loss suffered by the individual in the form of injury or death, or damage to other goods, land or buildings, that is caused by the safety defect. Manufacturers may also be separately liable to indemnify suppliers where the safety defect causes the supplier to breach a consumer guarantee.

Two defences are potentially available for AI system manufacturers: (a) the safety defect could not have been discovered at the time of supply because there was insufficient scientific or technical knowledge at that time (i.e. due to the black box nature of AI, manufacturers may be able to escape liability by claiming the AI systems are inexplicable); and (b) if the AI is part of a larger system (such as an autonomous vehicle), that the defect is attributable to the finished product or the combination of the AI component with other components, rather that the component itself.

Tort

Liability for damages caused by AI systems may also be established under tort law (namely, negligence) by establishing the usual elements of negligence (i.e., duty of care, breach, and causation). Considering the uncertainty as to how AI systems learn and make decisions, we expect it may be difficult for an applicant to establish causation. Generally, loss or damage that is reasonably foreseeable at the date of breach is recoverable.

Criminal

Given corporations are subject to criminal offences in Australia despite being non-natural entities, it is possible similar principles may be used to create another legal fiction to establish legal 'personhood to enable AI entities to be held criminally responsible for their actions. This creates obvious enforcement issues as to how to punish an AI entity that has no corporeal being.

More likely in our view is the introduction of amendments to legislation to create vicarious liability for the operators or creators of AI engines, more akin to vicarious liability for acts of employees or imputed knowledge of officers of a company. Often, these will require the particular individual to have actual knowledge of the likelihood of an adverse outcome from the use of the AI or was reckless as to that possibility.

This has the benefit of enabling access to the assets and personnel of a corporation for compensation and punishment purposes.

In all criminal cases, it is necessary to establish both the actus reus and means rea elements can be established against the AI entity (i.e., it was not a mere innocence agent), or if Parliament intervenes to legislate specific offences for AI entities or deem certain elements of offences as strict liability.

6. Who is responsible for any harm caused by an AI system? And how is the liability allocated between the developer, the user and the victim?

Because an AI system does not have separate legal status, it is the supplier of the AI solution who is most likely to be responsible for it. The supplier may be one of several parties, depending on the circumstances.

As discussed above in Question 5, under Australian Consumer Law, product liability regime manufacturers may be responsible for harm suffered due to safety defects in AI systems. Manufacturer is broadly defined and may capture various persons involved, including the developer, the manufacturer, and the ultimate supplier of the AI-embedded product.

Whether or not a software supplier (and, by extension, an AI provider) owes a duty of care to its end users has not yet been tested in Australian courts. If a duty of care is found, we would generally expect it to apply to the downstream supplier who makes the AI system available for use. However, there have been suggestions that tort law should be developed to impose strict liability on the 'owner' of an AI system.

The user of an AI tool may also have liability for their own conduct using an AI system under online safety or criminal laws (as discussed above in Question 5). For instance, if an individual uses an AI tool to create 'deep fake' image-based abuse content, that behaviour is itself

 © 2023 Legalease Ltd

criminal, irrespective of whether an AI tool is involved, and it is unlikely in our view that the supplier of the AI tool would in that case have liability (unless the tool was specifically designed for or is marketed for that purpose). We also note that under many AI providers disclaim all liability for use of the AI system and require the user to indemnify the AI provider for liability arising from the users' use of the services, including any user generated content. These clauses have not yet been tested in Australia but are unlikely to be effective to the extent they allow providers of AI tools or AI-based services to escape the financial implications of normal, foreseeable real-world uses of their tools and instead pass them on to individual (and lawful) end users.

7. What burden of proof will have to be satisfied for the victim of the damage to obtain compensation?

Australia does not have any AI-specific legislation that shifts the burden of proof, which will depend on the nature of the claim. Generally, the burden of proof will lie with the victim of the damage.

- **tort**: the claimant is responsible for proving the existence of a duty of care, breach, causation and reasonable foreseeability on the balance of probabilities. The additional element of fault required to establish negligence may pose particular challenges for injured claimants, given the highly technical processes in which AI systems are 'manufactured';
- **product liability**: under the ACL's product liability regime, the consumer bears the burden of proving, on the balance of probabilities, that the product was defective and that the damage was caused by the safety defect; and
- **criminal**: the burden of proof will generally lie with the prosecution.

8. Is the use of artificial intelligence insured and/or insurable in your jurisdiction?

Many AI risks will fall within existing policies, including:

- cyber – data loss, data breaches;
- product liability – defective AI products that cause injury or property damage; and
- professional indemnity – AI caused negligence or errors (e.g. algorithmic bias claims);

To date, we are not seeing specific AI endorsements (i.e. AI exclusions) yet but we note the way Cyber Property and Data Exclusion Endorsements might come into play on general insurance policies. Separately, we are starting to see specific coverage for artificial intelligence solutions, covering risks such as model performance.

9. Can artificial intelligence be named an inventor in a patent application filed in your jurisdiction?

No, in *Commissioner of Patents v Thaler* (2022) 289 FCR 45, the Australian Federal Court held that under the *Patents Act 1990* (Cth), a patent for an invention can only be granted to an inventor that is a natural person. The question of whether an AI system with a human inventor, could satisfy the necessary element of inventorship, remained undecided. The High Court of Australia denied an application for special leave to appeal this decision, and as such the Full Court's decision currently prevails in Australia (i.e., an AI system cannot be listed as an inventor of a patent in Australia, only a natural person), while leaving the door open for future questions surrounding AI creation and authorship.

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

Section 32 of the *Copyright Act 1968* (Cth) provides that copyright subsists in original works. The High Court of Australia has offered clarity as to when a work is 'original', suggesting originality requires a human author who has exercised independent intellectual effort. Accordingly, an image generated purely by AI does not benefit from copyright protection in Australia.

Arguably, images generated by AI may be afforded copyright protection if there was sufficient human oversight and intervention in the image generation process (e.g., if an individual provides detailed and continuously refined instructions). This would need to be decided on a case-by-case basis by the courts.

Interestingly, the requirement of human authorship does not apply to copyright in subject matter other than works (i.e., films, sound recordings, published editions and broadcasts). Instead, copyright ownership attaches to the entity that undertook the "making" or "publishing" of the work. If similar protection were to apply to works created by AI, then this would suggest that the manufacturer or producer, or rather the programmer, of the AI could be considered the author of the work.

 © 2023 Legalease Ltd

11. What are the main issues to consider when using artificial intelligence systems in the workplace?

The main issues to consider when using artificial intelligence systems in the workplace include:

- **confidentiality and data security**: data uploaded to third party AI service providers may not be confidential or secure, including where the data input and the AI generated output are used to retrain the AI model. Agreements with the AI service provider should be in place clarifying data ownership, retention, and use.
- **accuracy and reliability**: AI-generated information may not always be accurate or complete – a phenomenon known as 'hallucination'.
- **transparency and explainability**: AI decision-making is often opaque and inexplicable – known as the AI black box problem. This is particularly harmful when AI is used to make significant or irreversible decisions that impact individuals, because it makes it difficult for individuals to challenge decisions when it is not known why they were made. Further, the black box effect makes it impossible to validate AI outputs, reducing the ability to ensure AI accuracy.
- **algorithmic bias**: AI models are only as good as the data they are trained on: if the training data is biased or incomplete, the AI system will these perpetuate biases. When used for instance to make hiring decisions, there must be separate processes in place to ensure alignment with workplace values and anti-discrimination laws.
- **employee surveillance**: Several jurisdictions have specific employee monitoring laws, and some have general surveillance laws that apply to workplace surveillance which, broadly speaking, impose obligations to notify staff of surveillance activities, in some cases to consult with them before commencing, and to have policies in place explaining the limits of the surveillance activities.

12. What privacy issues arise from the use of artificial intelligence?

The use of AI raises a number of privacy issues, most notably:

- **data collection**: AI has the potential to enable widespread collection of personal information at an unprecedent scale. The discussion on the case of *Clearview AI Inc and Australian Information Commissioner* [2023] AATA 1069 (see question 15 below) demonstrates the privacy issues in using AI to web scrape personal information. After being trained, an AI system may have the capacity to collect personal information for its operations (for instance, prompts into ChatGPT could include personal information);
- **data use**: see below the rules applicable to the use of personal data to train artificial intelligence systems;
- **data minimisation**: AI solutions are trained on large datasets, which is necessarily in tension with the data minimisation principle underlying privacy protections;
- **data quality**: given the vast quantity of personal information AI can be trained on (and infer), it is impracticable to ensure the personal information is accurate, up-to-date and complete;
- **lack of transparency**: the black box problem of AI means it is difficult to determine what personal information is being used and how (including whether complete or biased datasets are being ingested);
- **inference and prediction**: AI has the ability to infer or predict personal or sensitive information about individuals, even if that information was not explicitly provided to the system (and whether that information is true or not); and
- **re-identification**: there are risks of re-identification of de-identified personal information due to artificial intelligence capabilities.

13. What are the rules applicable to the use of personal data to train artificial intelligence systems?

In Australia, the *Privacy Act 1988* (Cth) (**Privacy Act**) regulates the collection, holding, use, and disclosure of personal information by Australian government entities and private sector entities.

There are 3 key considerations:

- is the collection of personal information reasonably necessary for the organisation's functions or activities?
- is there notice to and consent by the individual, or would the individual reasonably

 © 2023 Legalease Ltd

expect their personal information to be used in that way?
- is the personal information then used for that purpose?

While collecting personal information may be reasonably necessary to train AI systems (although not if de-identified data would suffice), it is unlikely individuals have consented to, or would reasonably expect that, their personal information being used to train artificial intelligence.

Additionally, APP entities must take reasonable steps to ensure the personal information they collect, use, or disclose is accurate, up-to-date and complete. Accordingly, it would be necessary to take reasonable steps to ensure the accuracy of any personal information used to train artificial intelligence systems.

An alternative is to de-identify personal information before it is ingested into an AI solution – in Australia (and as distinct from other jurisdictions which wee de-identification as a form of processing that itself requires relevant consents) once de-identified, the information ceases to be 'personal information' provided it is not capable of re-identification.

14. Have the privacy authorities of your jurisdiction issued guidelines on artificial intelligence?

Yes, the Office of the Australian Information Commissioner (**OAIC**) (Australia's privacy regulator) issued its Guide to Data Analytics and the Australian Privacy Principles in March 2018 (see here).

On 16 February 2023, the Attorney-General's Department released its large-scale privacy review, the Privacy Act Review Report (**Privacy Review**) which included the following recommendations relating to AI:

- **targeting**: include clear information about the use of algorithms and profiling to target individuals (tailoring services, content, information, advertisements or offers). This will be particularly problematic for artificial intelligence due to its transparency and explainability difficulties;
- **automated decisions**: provide information:

1. specifying the types of personal information that will be used in automated decisions; and
2. how such decisions are made;

- **privacy policies**: include information about the use and types of personal information to make substantially automated decisions with legal or similarly significant effect; and
- **collection**: define 'collection' to cover information obtained from any source and by any means, including inferred or generated information. This includes data generated using data analytics and machine learning.

15. Have the privacy authorities of your jurisdiction discussed cases involving artificial intelligence?

In *Clearview AI Inc and Australian Information Commissioner* [2023] AATA 1069, the Administrative Appeals Tribunal (**AAT**) partially affirmed the OAIC determination that Clearview had breached Australian privacy laws by using an AI-driven web crawler to scrape images and data from publicly available websites (the data was then used to offer facial recognition services). The AAT found that Clearview had failed to take reasonable steps to implement practices, procedures and systems to ensure compliance with the APPs and had collected sensitive information without consent. However, the AAT rejected some findings of the OAIC, and concluded there was no breach of the following:

- APP 3.5, because:

1. online information was publicly available to take without informing the relevant individual; and
2. where there is no access restriction on online information, it is not unfair to collect that information (noting it may be different if collection was in breach of a website's terms of service);

- APP 5.1, because its was impracticable to notify individuals due to the quantity of personal information that was scraped without individuals' knowledge; and
- APP 10.2, because the data was as accurate as Clearview could provide in the circumstances (even if the public information was not accurate or up to date at the time of collection).

In *Commissioner initiated investigation into 7-Eleven Stores Pty Ltd (Privacy) (Corrigendum dated 12 October 2021)* [2021] AICmr 50, the OAIC found 7-Eleven had breached the Privacy Act by collecting sensitive information without consent and without taking reasonable steps to notify individuals about the collection of their personal information. 7-Eleven had deployed third-party facial recognition technology for in-store customer surveys, which captured facial images,

 © 2023 Legalease Ltd

created faceprints and 'cross checked' responses on customer satisfaction surveys with the facial expression of the individual to determine the accuracy of the responses. Additionally, the OAIC found the extensive collection of sensitive information was not reasonably necessary for 7-Elevens' functions and activities, here being to improve customers' in-store experience.

16. Have your national courts already managed cases involving artificial intelligence?

Yes, as referred to above, in *Commissioner of Patents v Thaler* (2022) 289 FCR 45, the Full Court of the Federal Court of Australia held that artificial intelligence could not be an 'inventor' for the purposes of the *Patents Act 1990* (Cth) because an inventor must be a human.

There are currently no other cases considering artificial intelligence in Australia.

17. Does your country have a regulator or authority responsible for supervising the use and development of artificial intelligence?

There is currently no regulator or authority responsible for supervising the use and development of AI in Australia. The Australian Human Rights Commission Human Rights and Technology Final Report (2021) recommended establishing an AI Safety Commissioner to promote safety and protect human rights in the development and use AI in Australia.

18. How would you define the use of artificial intelligence by businesses in your jurisdiction? Is it widespread or limited?

The use of AI in Australia is widespread and spans across many sectors. The CSIRO recently released the *Australia's AI Ecosystem Momentum Report* (see here). The Report found that 60% (of 200) respondents are accelerating their use of AI, and found the following industries were leading in the use of AI for decision-making in Australia:

- Financial services (14%);
- Professional services (12%);
- Technology (11%);
- Healthcare (7%); and
- Telecommunications services (7%).

The Australian Government is prioritising AI development in the healthcare sector, with substantial investments being made, including $19 million in grants for healthcare projects involving AI. Government AI initiatives in healthcare are paralleled in the private sector. For example, Harrison.ai has raised approximately $120 million to develop AI healthcare technology such as an AI tool for radiology scans.

However, while AI use by businesses generally is accelerating, we have definitely seen a global pullback in the number of businesses using generative AI since the advent of ChatGPT in November 2022, with many publicly banning the use of generative AI for their employees (e.g. Amazon, Goldman Sachs, PWC, Apple).

19. Is artificial intelligence being used in the legal sector, by lawyers and/or in-house counsels? If so, how?

Yes, AI is being used in the legal sector. This includes for:

- contract generation automation;
- eDiscovery;
- due diligence;
- contract analysis;
- research; and
- drafting articles.

Currently, law firms are driving a lot of these initiatives, as they are best suited to benefit from large scale operational efficiency improvements and have the resources to develop tailored and unique AI solutions. Until cheaper and more legal-specific AI solutions are developed and commoditised, in-house counsel may find it difficult to leverage AI. Publicly available AI models such as ChatGPT are currently being used by both private practice lawyers and in-house counsel.

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

5 key challenges raised by AI for lawyers in Australia are:

- **Hallucination**: AI models may fabricate facts and sources without indicating whether they have falsely created this information. Further, it is difficult to determine whether the AI model is providing a factually correct answer, and in most cases, this requires external validation (reducing the efficiency of using AI).
- **Lack of Legal Knowledge**: AI

 © 2023 Legalease Ltd

models are only as good as the data they are trained on. This means AI may not provide a reliable, complete, or accurate interpretation or application of the law because lots of legal material is not publicly available and so the training dataset may not contain sufficient data on specialist areas of law.
- **Confidentiality and Legal Professional Privilege**: data uploaded to AI (including prompts) may waive confidentiality and legal professional privilege. Further, as with any third-party service provider, there is an increased risk of data breaches when uploading sensitive client information to external AI providers. Lawyers need to ensure appropriate controls and processes are in place to protect client information.
- **Technology Competency**: using AI as co-pilots to drive efficiency requires lawyer to interact with AI technology. Accordingly, lawyers will need to become AI literate, as well as understand the functionality and limitations of AI, to leverage the power of AI.
- **Lack of Guidance**: Australia, like most countries globally, currently lacks regulatory guidance on the use of AI. This makes using AI in legal services a grey area as firms and lawyers need to identify and mitigate the risks of using AI themselves. While many AI use cases will be appropriate, it remains to be seen where the boundaries will be drawn.

5 key opportunities raised by AI for lawyers in Australia are:

- **Increased Efficiency**: AI can handle routine and time-consuming tasks such as due diligence or populating templates, allowing lawyers to focus on more complex issues and strategy.
- **Improved Access to Legal Services**: AI-powered chatbots and applications can provide basic legal advice, making legal services more accessible to those who might not be able to afford full legal services.
- **Data Analysis**: AI can help lawyers analyse large volumes of data quickly and accurately. For example this can aid in case strategy by analysing a judge's history of rulings, the track record of opposing counsel or the value of damages awarded.
- **Cost Reduction**: by automating routine tasks, AI can reduce costs, making legal services more affordable and competitive.
- **Learning**: AI will automate repetitive, administrative work, allowing junior lawyers to start developing substantive knowledge and important skills such as critical thinking earlier in their career. For more senior lawyers, AI can be leveraged as a creative partner such as by helping generate and test novel arguments. It can also be used to help keep abreast of information about clients and other market participants.

21. Where do you see the most significant legal developments in artificial intelligence in your jurisdiction in the next 12 months?

In the next 12 months, significant legal developments in artificial intelligence will likely involve:

- **Governance Framework**: On 1 June 2023, the Australian Government released an AI Discussion Paper (see here), seeking submissions on the mechanisms available to govern AI, as well as feedback on the proposed risk-based approach to AI governance. In the next 12 months, it is likely we will see the Government's response and potentially some draft legislation establishing an AI governance framework.
- **Legal Personality of AI**: As AI becomes more sophisticated, independent, and plays a more significant role in society, the issue of whether AI has some form of legal personality will likely need to be resolved.
- **Liability for AI Actions**: who is responsible if an AI causes harm? The current Australian legal framework may need to adapt, or at least be clarified, to hold someone (e.g., the AI developer, user, or owner) responsible for damages caused by an AI. In Australia, we

 © 2023 Legalease Ltd

may see legislation like the draft EU AI Liability Directive, which will create a rebuttable presumption of causality between breach of a duty of care and the AI output that gives rise to the relevant damage.

- **Intellectual Property Rights**: AI has the potential to create or invent products and works independently, raising important questions about IP rights. Australian IP law will likely need to be clarified to determine ownership issues in relation to AI-generated creations. Further, the use of AI in processing and analyzing vast amounts of data can potentially infringe on existing IP rights, a concern that will need to be addressed.
- **Privacy and Data Security**: it is likely we will see the Government's response to the Privacy Review and potentially some draft legislation. This will likely address some of the unique challenges posed by AI, such as complex data collecting and processing, algorithmic decision-making, potential bias, and heightened data security risks.

Contributors

Alex Hutchens
Partner
ahutchens@mccullough.com.au

Rebecca Lindhout
Senior Associate
rlindhout@mccullough.com.au

Sebastian Galetto
Lawyer
sgaletto@mccullough.com.au

Alex Komarowski
Lawyer
akomarowski@mccullough.com.au

 © 2023 Legalease Ltd