www.pwc.com.au

Artificial intelligence: What directors need to know

Artificial Intelligence
Accelerate Responsibly

August 2023

pwc

The era of AI has well and truly begun...

With generative AI tools like ChatGPT well and truly becoming an 'overnight' sensation, many have been awakened to the potential for AI to revolutionise the way we do business. But the truth is that the use of AI technologies in everyday business functions is already commonplace. From Netflix using AI to recommend movies based on what we have previously watched, to the Commonwealth Bank of Australia using AI to detect suspicious and unusual banking behaviour on its digital platforms[1], AI is already disrupting traditional business.

In light of the staggering increase in AI use, directors are under mounting pressure to ensure their organisations are prepared to use AI in a responsible manner. But what does this really mean in practice?

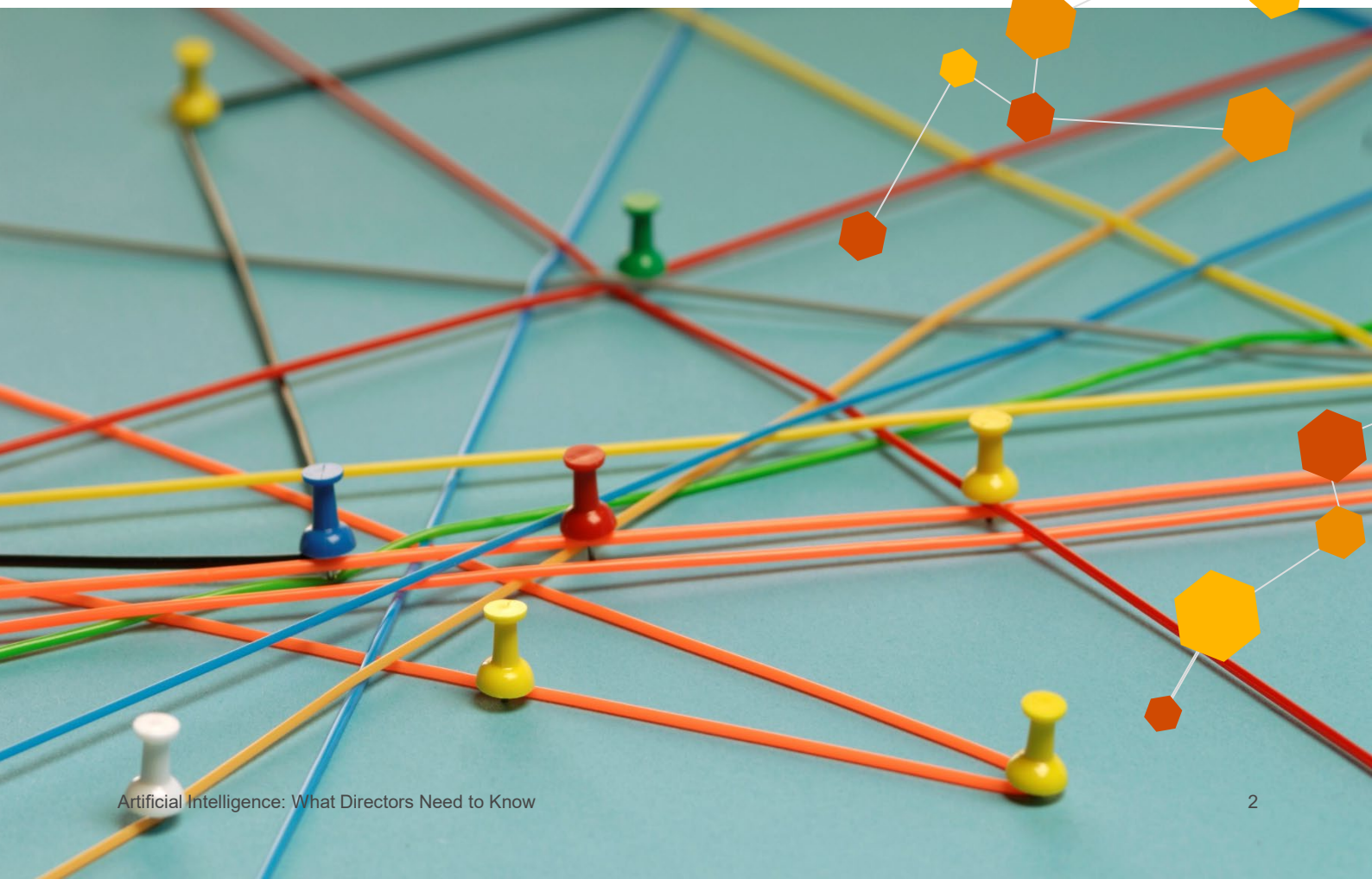
Although specific black letter law regulating AI has yet to be formalised, directors need to understand their role and responsibilities in the deployment of AI. In short, that means implementing AI governance.

Australian laws have yet to clearly define what AI is, let alone what a director's duties are when it comes to AI. But it could very well be on the horizon, with the Australian Government recently releasing a Discussion Paper on 'Safe and responsible AI in Australia'.

AI is happening *now*, and directors should look to stay ahead of the curve. The choice is not between using AI and not using AI. Given its prevalence and trajectory, AI will either be used by an organisation governed or ungoverned – the choice is for the directors to make.

This article looks to unpack the relevance of directors' duties to AI and how directors can effectively manage these duties. AI, with all its promises and opportunities, comes with a range of known risks. Without appropriate organisational governance, there is a real risk that AI becomes a source of harm and risk (and therefore, liability) to any business.

1 Commonwealth Bank of Australia, 'CBA introduces leading AI technology to protect customers from scams', *Newsroom* (Web Page, 4 July 2022) <https://www.commbank.com.au/articles/newsroom/2022/07/scams-fraud-artificial-intelligence.html>.



Key takeaways

Given contemporary trends in AI use in the workplace, understanding the technology and its impacts in the organisation and the boardroom falls directly within the remit of a director's obligation to exercise due care, skill, and diligence in discharging his or her duties.

As such, directors must:

Examine legal and regulatory consequences

Despite lack of explicit AI law, legal obligations may arise from existing governing legislative instruments or regulations eg privacy, human rights, or anti-discrimination laws. Directors should be aware of how the use of AI in their organisations may contravene these laws, and ensure mitigating processes are put in place to manage compliance.

Implement appropriate AI governance

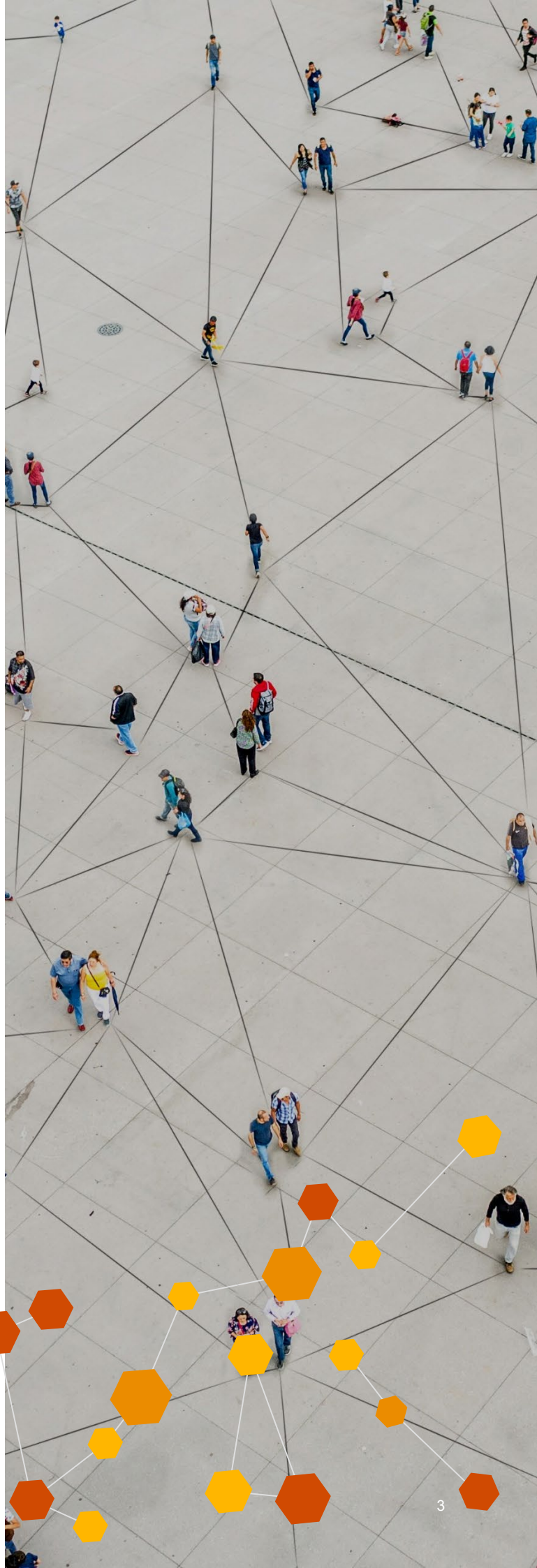
AI requires boards' attention because it affects every aspect of their oversight duties. Directors and officers must consider how to manage the data, models and people involved in implementing AI. Critically, directors cannot govern risk effectively for their organization in the modern world without dealing with AI.

Consider the risks of harm of AI use

Consider the impact of the use of AI on society, people and your organisation. Risks to your organisation can be commercial, regulatory and reputational in nature. In particular, consider the impact on your organisation's key stakeholders such as your employees and customers. Consider also the risks of not adopting AI solutions.

Ensure ongoing assurance of AI

Like any other business risk, AI is not a 'set and forget' obligation – routine assurance of AI systems, and the governance framework itself, is required to ensure compliance with regulation and best practice.



How do director duties extend to AI?

Under the *Corporations Act 2001 (Cth)*, directors have a general duty to exercise their powers and discharge their duties:

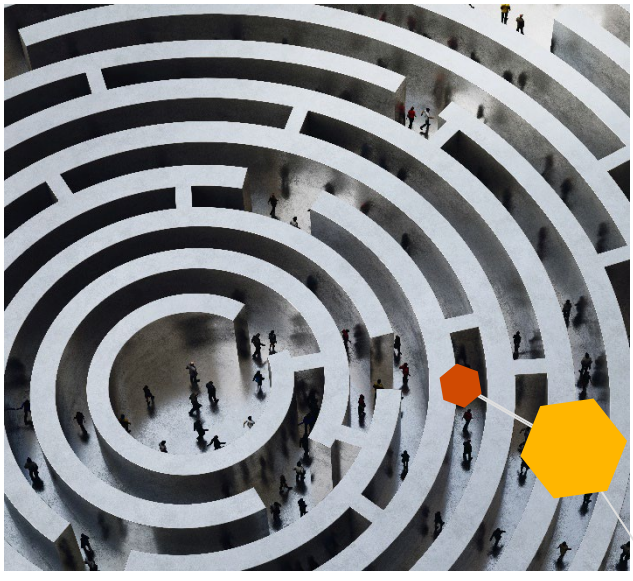
- in good faith including acting in the best interests of the company and for a proper purpose;[2]
- with reasonable care and diligence;[3] and
- without using their position or information to gain personal advantage.[4]

The Federal Court of Australia has outlined that these responsibilities embedded are not limited to statutory duties, but also extends to the 'equivalent duties at common law and in equity'.[5]

ASIC has already enforced cyber security resilience obligations on directors to ensure that companies appropriately manage cyber security risk. But significantly less has been said about what a director's obligations may be in relation to a company's adoption of AI. Whilst cyber security risk is one component of AI use, there are a range of other significant risks that AI poses to a company, its people and society more broadly.

While "reasonable care and diligence" is not defined under the Act, it can be determined by assessing the foreseeable risk of harm against the probable benefits that may be expected to flow to the company.[6] This includes the requirement to implement good governance procedures and to not knowingly do anything that would expose the company to a forseeable risk of harm (such as financial harm, damage to reputation, etc.) where it does not outweigh the potential benefits to the company.

In a world where phrases like "ChatGPT" and "Generative AI" are commonplace, it is not unreasonable to suggest that there is an expectation for directors to be both technology and AI-literate in order to effectively exercise their powers and discharge their obligations.



Can directors be held liable for improper use of AI in a company or AI 'gone wrong'?

The short answer is yes.

Directors could be exposing the company to legal liability if they fail to uphold their statutory duties and mitigate preventable harms arising from AI systems created and used by the companies they oversee.

Through the 'stepping stones' principle, liability may be imposed onto directors personally in certain circumstances. Under the 'stepping stones' principle, a company contravention of a law or failure to manage risk of non compliance can result in the establishment of personal liability where the director fails to implement appropriate measures to govern and manage those risks. There is no need for proof of 'involvement' by the director in the actual breach itself. In that regard, imposition of personal liability on a director in AI-related harm is a real possibility.

This view is echoed in current enforcement trends in cybersecurity. As seen recently is *ASIC v RI Advice Group* [2022] FCA 496, the Federal Court rendered a director personally liable for not preventing a foreseeable cyber security risk – the Court considered that there was an indirect breach of directors' duties.

Case study: *ASIC v RI Advice Group*

In a landmark decision, the Federal Court of Australia has determined that a financial services company failed to have adequate risk management systems in place to manage cybersecurity threats.

In focusing on the conduct of the directors and officers of RI Advice Group, the Court held that their conduct contravened their statutory duty of care under s 180(1) of the Act by exposing their company to a risk of harm.

As recognised by Rofe J, in a dynamic market where there is increasing reliance on technology and digital platforms to deliver financial services, "cybersecurity risk forms a significant risk connected with the conduct of the business."

This could easily be applicable to the industry's next 'big thing', AI. In light of Rofe J's comments, directors and officers should be seeking to take reasonable steps to respond to, and reduce, risk in order to avoid breaching their duty of care.

2 *Corporations Act 2001* (Cth) s 181.
3 *Corporations Act 2001* (Cth) s 180.
4 *Corporations Act 2001* (Cth) s 182 and s 183.
5 *Cassimatis v Australian Securities and Investments Commission* [2020] FCAFC 52, 29.
6 Australian Institute of Company Directors, *Catch a Falling Star* (Web Page 1 February 2023) <https://www.aicd.com.au/board-of-directors/duties/liabilities-of-directors/catch-a-falling-star.html>.

The risks of AI

The exponential growth in the accessibility to, and capability of, AI solutions presents profound opportunities and risks for organisations, people and society at large.

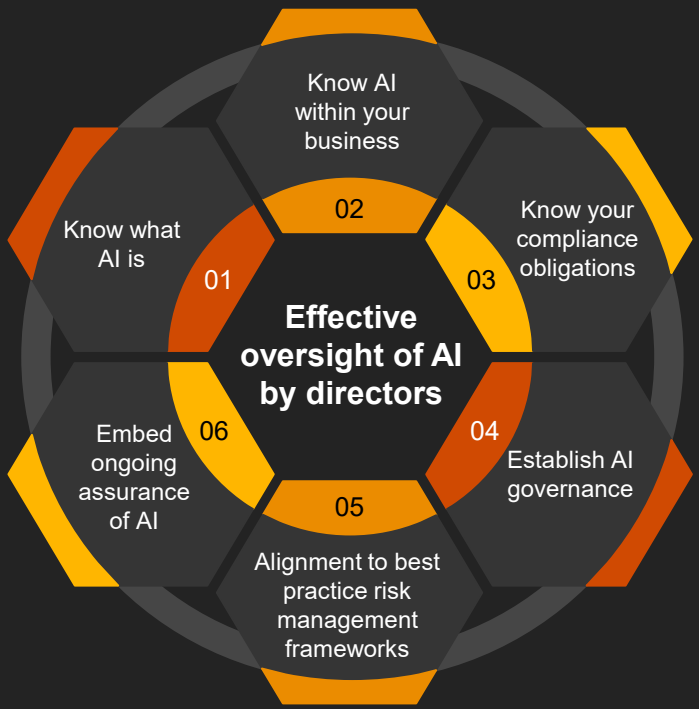
With each new opportunity that AI unlocks, it also brings about a new breed of issues and challenges from operational risk management, ethics and morality and legal standpoints. For example:

- Creating and using AI and related technology can present unique intellectual property issues regarding ownership of AI, IP protection through copyright and other IP regimes, and infringement of such IP.
- There is the fundamental question of privacy – there is a heightened risk of non-compliance with data protection and privacy regulation (eg unlawful use of personal data or failure to secure that personal information if cyber security controls in the AI tool and not effective) due to the size and complexity of utilised data sets.
- Unlawful discrimination or harmful biases caused by imbalances in training data and/or incomplete review of model outputs. Algorithmic bias in AI used for decision-making (eg hiring decisions) could lead to a potential breach of anti-discrimination laws.
- While the benefits of AI from a commercial perspective are clear, its use in setting prices and responding to market changes raises potential antitrust risks, in addition to lending itself to potential unlawful, anticompetitive agreements in its operation and use.
- Operational disruptions due to insufficient planning for continuity and resilience for business critical applications of AI.
- Malicious use of AI leading to cyber attacks, fraud and circumvention of security controls.
- Reputational damage by failing to meet community expectations around the use of AI in products/ services, and the use of personal data with AI.
- Over-reliance on AI for automation (eg applying the wrong types of models to use cases, or inadequate human review and output verification).
- Failure to respond to advancements in artificial intelligence, exposing the organisation to business model disruption.
- Misinformed decisions or inaccurate insights due to quality issues with training data, model design or improper application/usage of a model.

So, now what?

Appropriate AI governance can, if done correctly, accelerate the growth of a company's uptake and ability to benefit from AI solutions, and ensure directors and officers meet their obligations under the Corporations Act.

Set out below is a *list of key activities* that directors should consider for them to be able to effectively oversee the implementation of a good AI corporate governance framework within their company. This doesn't require organisations to reinvent the wheel, in fact, many organisations have existing governance and risk management processes and procedures that can be leveraged to effectively govern AI within the organisation. The trick is identifying those most relevant and augmenting them as required to address the uniqueness of AI solutions.



Key activities directors should consider to effectively implement and oversee governance of AI

01 Know what AI is

AI is a nebulous concept. Directors need to consider what the company considers to be "AI" for the purposes of its AI governance and establishing appropriate guidelines for AI. Even subtle variances in definition can have major impacts on its application in the organisation. For example, your definition could go as broad as all automated decision systems, or it could be narrowed down to focus on a field of AI (eg unsupervised deep learning) or a type of AI (eg Generative AI). As a result, it is critical to ensure a functional definition of "AI" is established that reflects the scope that is to be governed.

Some commonly used definitions of AI include:

CSIRO – Artificial intelligence (AI) may be defined as a collection of interrelated technologies used to solve problems autonomously and perform tasks to achieve defined objectives, in some cases without explicit guidance from a human being.[7]

EU AI Act – 'Artificial intelligence system' (AI system) means a machine-based system that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate output such as predictions, recommendations, or decisions influencing physical or virtual environments.[8]

OECD – [An] Artificial Intelligence (AI) System is a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments.[9]

While directors are not necessarily expected to become digitally-literate in the sense that they must learn how to code or create AI models themselves, there is a duty for a director in the current day and age to be properly advised on data and technology. As such, failure to understand their company's use of AI technologies could give risk to a risk of breach of their duties as a company director.

7 CSIRO, 'Consultation Hub' Mapping Australia's Artificial Intelligence and Autonomous Systems Capability (Web Page, 2 October 2020) <https://consult.industry.gov.au/mapping-australias-artificial-intelligence-and-autonomous-systems-capability>.
8 The EU Artificial Intelligence Act, The EU Artificial Intelligence Act (Web Page, 14 June 2023) <https://www.artificial-intelligence-act.com/>.
9 OECD.AI Policy Observatory, OECD AI Principles Overview (Web Page, May 2019) <https://oecd.ai/en/ai-principles>.

02 Know AI within your business

Hand in hand with the need to come to a consensus on the definition of AI is the need to understand how AI operates, or is going to operate, in the business.

Directors need to understand the specific type of AI technology captured within the parameters of the business in order to effectively establish a structure which governs and mitigates risks relating to AI. Different AI technologies and their applications will present differing risks that require tailored strategies to mitigate - for instance, Large Language Models (LLMs) hallucinate, posing risks in resiliency and explainability, while autonomous decision-making AI functionalities may pose risks in safety, transparency and accountability. Mitigating these risks requires understanding their interaction with the business's use case and applying relevant controls and monitoring.

Machine Learning Systems – a complex set of machine learning models that collects and uses existing data to develop outputs on new data

Generative AI – system that generates various types of content, including text, imagery, audio and synthetic data in response to prompts. (e.g ChatGPT)

Expert systems – a computer-based decision-making system that is capable of solving complex problems in specific domains/areas of expertise. Expert systems can advise, diagnose, instruct and assist humans in decision-making, predict results, interpret input, suggest alternatives, amongst other capabilities.

Natural language systems – systems that are able to undertake natural language processing (NLP). Organisations use NLP to read text, hear speech (voice to text), interpret and analyse language-based data, measure sentiment, and determine which parts are important.

Automated decision-making systems – systems that are capable of making a decision by an automated means and without human involvement. The systems can process and analyse large-scale data from various sources to make the decision. It is becoming widely used in public administration eg by governments, in business, health, education, law and other sectors, with varying degrees of human intervention or oversight.

FRT (Facial Recognition Technologies) – any system or device that is capable of determining whether an image contains a face. Often FRT uses biometric data to verify someone's identity, to identify an individual or to analyse characteristics about a person.

Virtual agents and chatbots – chatbots are rule-based software that has been designed to understand and respond to select human keywords or phrases. Virtual agents advance the chatbot functionality – using AI, including natural language processing, to recognise human speech.

Recommendation systems – systems that suggest products, services, information to users based on analysis of data, patterns and trends.

AI-powered robotics – 'robots' or physical systems that are equipped with various sensors eg proximity, computer vision to move and execute tasks in dynamic environments.[10]

A director should look to understand at a high level:

- **AI Technology/Model** – What is the underlying AI technology and how does it work?
- **AI Use Case Benefits** – What is AI being used for within the business? What are the benefits to the organisation through the use of AI?
- **AI Use Case Risks** – What are the key risks to the organisation through the use of AI? What data is being used to train (or retrain) the AI model? What data is provided to the model for inferencing or prompting purposes? Are compensating controls required to achieve the level of precision that the use case requires?
- **Likelihood of impacts to individuals ad groups** – What is the output of the AI model and its level of precision? What are the downstream impacts if AI goes wrong for stakeholders and society more generally?

10 Lauren Solomon, Nicholas Davis 'The State of AI Governance in Australia' (2023) *Human Technology Institute* 11.

03 Know your compliance obligations

With AI developing so rapidly, it is no surprise that specific black letter law regulating AI is still playing 'catch-up'. However, in recognition of AI becoming critical to many organisations' operations, governments all around the world are moving swiftly to adapt to the emergence of new AI capabilities.

Some examples include:

- The European Union lawmakers have passed a draft of the Artificial Intelligence Act which would be the world's first set of wide-ranging laws related to AI regulation (set out on page 11).[11]
- At the end of March, the UK Government published a White Paper setting out how it proposes to approach AI regulation.[12]
- FSingapore launched A.I. Verify, the world's first AI Governance Testing ramework and Toolkit for companies to demonstrate responsible AI.[13]

Whilst there has been some consideration of AI in the context of privacy law reforms, and the release of an initial discussion paper on AI and the development of the optional AI Ethics framework, Australia has made no specific attempt at designing legislation that deals with AI. However, the recent release of a second discussion paper on the safe and responsible use of AI in Australia suggests that AI is definitely on the mind of the legislature.[10] The paper canvasses existing regulatory and governance responses in Australia and overseas, identifies potential gaps and proposes several options to strengthen the framework governing AI.

The question remains as to whether Australia will develop a new bespoke AI law (akin to the EU) or attempt to amalgamate it within existing laws, such as the federal *Privacy Act 1988* (Cth), cybersecurity legislation like the *Security of Critical Infrastructure Act 2018* (Cth) or Australia's various federal and state surveillance laws.

Regardless of approach, directors will need to be sensitive to the regulatory landscape surrounding AI globally. Directors should consider undertaking a regulatory scan to determine applicable laws and how they might impact on the organisation's use of AI prior to implementing any form of AI governance (discussed on page 13). This scan will assist directors in ensuring that the AI functionality does not breach any of their individual obligations or the obligations of their company.

Privacy and cyber security

There is a slew of privacy issues raised by the use of AI, particularly in the area of consent and the incorporation of personal information in AI modelling and inputs. Organisations must consider how AI will de-identify personal information, as well as an individual's right to erasure under the GDPR (and potentially the Privacy Act if those reforms go ahead).

Unrestrained by law or ethical concerns, cyber criminals are using AI to develop new innovative ways to exploit and attack technology systems. Directors must also ensure appropriate implementation, and ongoing monitoring, of cyber security measures in their business where large data sets are being utilised to train AI models.

Surveillance and tracking

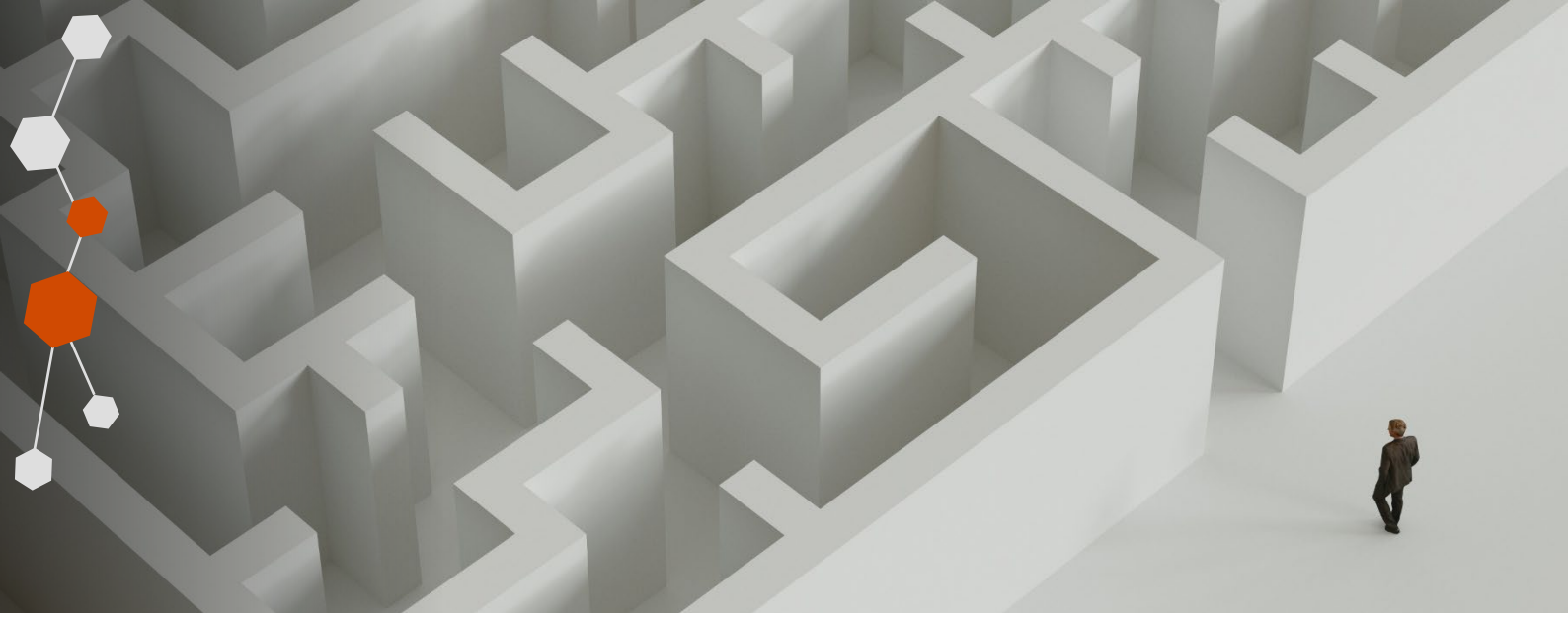
AI-based surveillance systems have the potential to revolutionise law enforcement and security, but they also pose significant risks to individuals' privacy. Facial recognition technology has been increasingly utilised to surveil and track people whether indirectly as part of traffic monitoring, or deliberately to assess OHS standards (eg monitoring signs of fatigue or intoxication in drivers using work vehicles) or to locate criminals. To the extent that these tracking and surveillance systems are being used, care must be taken to ensure compliance with existing surveillance legislation (eg *Surveillance Devices Act 2004* (Cth) and other state-based laws), individuals' rights to privacy and broader human rights standards.

Intellectual property (IP)

The complexities surrounding AI and IP are innumerable, from both a data input and output standpoint. In understanding what data is being scraped and used by AI, directors must ensure there are procedures in place to verify the source of input data to ensure IP rights are not being infringed upon. A second question then arises upon output – who owns the AI technology and who owns the IP rights in works generated by the AI? There are already IP and AI cases before the courts to establish a precedent. For example: in the *Commissioner of Patents v Thaler* [2022] FCAFC 62, the Full Court concluded that AI could not be considered an 'inventor' and therefore, its creations could not be the subject of a patent.

However, as AI develops and becomes more 'human-like', our current IP laws may need to be reassessed, and directors should keep aware of such changes.

11 European Parliament, *'Press room'*, AI Act: a step closer to the first rules on Artificial Intelligence Act (Web Page, 11 May 2023) <https://artificialintelligenceact.eu/>.
12 Gov.uk, *AI regulation: a pro-innovation approach* (Web Page, 29 March 2023) <https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach>.
13 Personal Data Protection Commission Singapore, *Singapore's Approach to AI Governance* (Web Page, 25 May 2022) <https://www.pdpc.gov.sg/Help-and-Resources/2020/01/Model-AI-Governance-Framework>.



Work, health and safety considerations

From an operational perspective, directors must consider the potential detrimental effects on workers of using AI and big data to monitor and direct work performance.

There are work, health and safety laws that require organisations to ensure the health and safety of their workers and other persons. The deployment of AI systems may introduce undue physical and psychological harm to employees.

"People problems" arguably require "people solutions" – using technology to assess employees productivity (eg by way of using data to assess or predict employees' talents and capabilities, work outputs, judge states of being and emotions or looking for patterns across workforces of, for example, tendency to use leave or become sick) and subsequently make decisions about their performance will potentially expose the organisation's people to heightened structural, physical, and psychosocial risks and stress.

Directors must also consider the criticality of a human-rights based approach on labour regulation and the way their organisation engaged its workforce, including through enterprise/collective bargaining ie the ramifications of replacing people employed under enterprise bargaining agreements with AI systems.

The broader human rights and workplace law concerns surrounding fairness, accuracy and honesty in management decisions are very relevant. It is possible that contraventions by the company could result in directors being held liable for mistreatment, discrimination, or bias.

Consumer protection

The use of AI in the delivery of products or services to consumers will undoubtedly increase the market asymmetry and power dynamic between consumers and businesses.

Whilst our current Australian Consumer Law **(ACL)** was not designed with AI in mind, it certainly will apply to any businesses looking to deploy or promote AI-enabled products or services. Directors will need to ensure that their organisations consider compliance with ACL obligations - this is particularly important as previously flagged, individual directors may be held personally liable for breaches under the ACL.

For example:

- The ACL requires that all claims about your product or service must be true, accurate and able to be substantiated. Although AI can be difficult to fully understand (a 'black box', so to speak), any company promoting AI, or products and services which utilise AI, must not make false or overreaching claims about the capability, accuracy, or functionality of a product or service.
- It is unlawful under the ACL to engage in conduct, in trade or commerce, that is misleading or deceptive, or likely to mislead or deceive. If you choose to rely on AI functionality, then you must ensure you truly understand the model and include guardrails regarding truthfulness of outputs. Otherwise, you may find yourself in breach of the ACL, even if your actions were unintentional.
- Use of AI systems in trade or commerce must not result in unconscionable conduct. The fairness of AI in its decision-making is a highly debated topic, and for good reason given the risk of bias. Directors should take care to ensure AI does not breach the ACL in this regard.
- A person involved in trade or commerce must not make false or misleading representations about goods or services or engage in misleading conduct in respect of these goods and services. Any comparisons involving AI products vs other AI products or even non-AI products must be valid, reasonable, accurate and fair.

The reality is that the ACL designed to protect the 'weaker' party in transactions, and it is only a matter of time before regulators look to strengthen the ACL and insert guardrails that will look to add to protection for consumers against the dangers associated with the use of AI (after all, the ACCC has already used misleading and deceptive conduct provisions to deal with privacy issues). Directors should monitor this space closely to ensure their company implements processes to ensure compliance with the ACL at all times with regards to AI.

Competition considerations

It is undeniable that AI technology fundamentally changes the way companies and their directors make decisions, especially in terms of predictive analytics and the optimisation of the decision-making process. AI's ability to trawl through copious amounts of data, compare and extract information at rapid speeds and analyse consumer behaviour to target marketing activities arguably creates many challenges for the existing competition regulation. AI can facilitate collusion, lead to abuse of a dominant position, and reduce competitive pressure, which will affect competition in the market and raise new antitrust considerations. Further, the control and access to data for LLM training and the ownership of AI models also raises competition concerns. Directors must be careful when considering the use of AI in their organisation, especially decisions that impact on the market or go to exclusivity of the provision of AI solutions, so that they do not act in contravention of competition laws.

Duty of care and negligence

General principles of negligence could also apply in the case where AI has caused harm where a duty of care exists. For example: AI can be used by health care providers to diagnose patients for treatment – an accepted relationship where a duty of care exists. If an AI mis-diagnoses the patient, which then results in significant harm or injury to the person, there may be a redress under the law of negligence.

To minimise the chance of failing to assert proper care, directors should look to establish processes to sufficiently develop, test, monitor, and supervise any AI system. Any use of AI should be subject to a rigorous risk assessment to identify and mitigate foreseeable harms.

Think about Insurance – Whilst not strictly a compliance obligation, company directors should consider the impacts of AI on their existing insurance arrangements. It is possible that insurance policies do not appropriately consider cover an organisation's use of AI and therefore may not protect the company against certain events that you would ordinarily expect to be covered.

Workplace and anti-discrimination

AI-enhanced HR practices that assist organisations make hiring decisions has significant implications on discriminatory practices.

With the release of the Australian Government's consultation paper, 'Updating the *Fair Work Act 2009* to provide stronger protections for workers against discrimination', it is evident that AI is seen to be a potential vehicle for increased employee discrimination. Directors must ensure there are protections in place in their business to mitigate any instances of discriminatory practices built into, and resulting from, AI and other similar systems.

On the flip side, there may be cases of positive discrimination and inherent bias in input data sets used to train AI algorithms for organisations that are trying to enhance diversity and inclusion in their workplace. Those who claim AI removes all aspects of human biases on gender and ethnicity during recruitment are toeing a fine line. The reality is that AI tools are a technology 'black box' and it may be difficult to ensure fairness and accountability in using these models to make company decisions.

Directors should be mindful that regulation of using automated decision-making tools is likely on its way. In recognition of these emerging technologies in employment practices, New York City passed the Automated Employment Decision Tool Law, which makes it unlawful for employers to use automated decision-making tools to screen individuals for employment decisions unless certain parameters and risk mitigation measures are undertaken eg bias audits, data disclosure, and appropriate notification. It will be pertinent for directors in Australia to monitor regulatory developments and review the way hiring and promotion decisions are currently being made.

The EU AI Act: an example of where Australia may be headed in AI regulation…

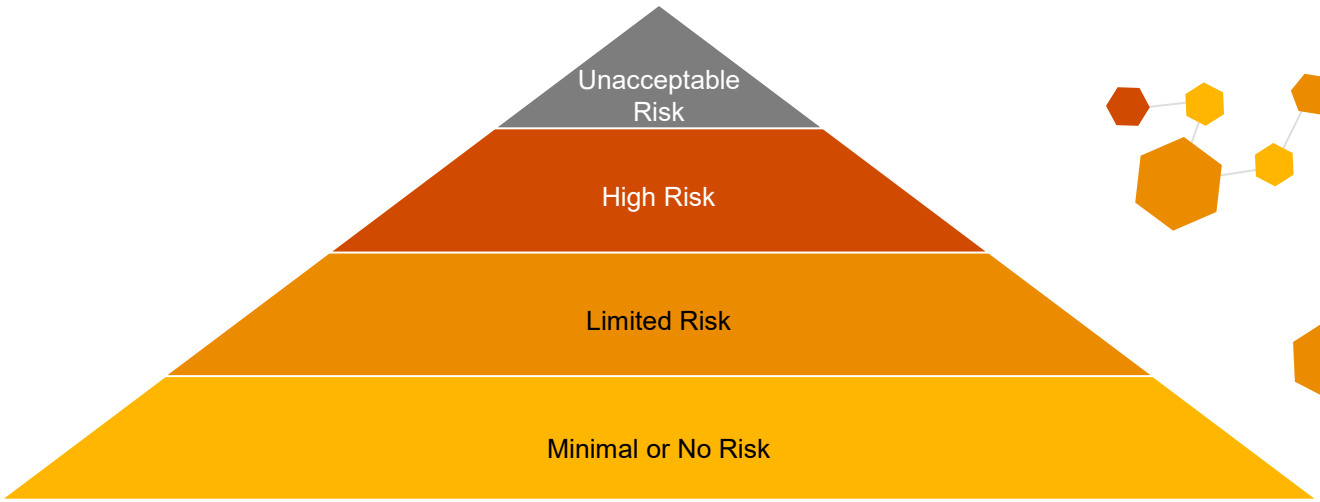
The EU Artificial Intelligence (AI) Act

- If passed into law, the EU AI Act will mark a huge milestone in AI regulation – it will be the world's first legislation that looks to regulate the development and use of AI generally.
- It is likely that Australia will, at least to some extent, look to the EU AI Act and its provisions in the drafting of its own AI regulation.

Key takeaways:

- The AI Act is intended to have an extraterritorial impact on the development and use of AI both within EU and overseas. It intends to regulate AI systems which are developed, used and sold within the EU, as well as AI systems that are used outside the EU but produce outputs that are used in the EU. Like the GDPR, if your organisation is or is going to use AI in the EU, this legislation must be considered.
- The AI Act employs a risk-based classification system that assigns a risk rating to the AI technology – each risk rating has associated regulatory obligations.
- There are four risk tiers proposed by the AI Act: unacceptable, high, limited and minimal.
  - AI systems that pose *Unacceptable Risk* are prohibited in the EU, with little exception.
  - Those that pose *High Risk* are subject to substantive and strict obligations under the AI Act.
  - AI systems that pose *Limited Risk* are subject to transparency and notification obligations.
  - AI systems that pose *Minimal or No Risk* can be used in the EU with no restrictions.
- There are enforceable undertakings linked to the AI Act, including significant penalties for breach and non-compliance with the AI Act.

As Australia continues in its discussions on AI regulation, organisations must remain aware that there are developments occurring in other jurisdictions eg the EU, that may also impact on its business.



04 Establish a good AI governance framework

In order to use AI tools responsibly, there is a need to establish a robust, holistic, and accessible governance framework that underpins the development, implementation, procurement and use of AI technologies.

As in *ASIC v RI Advice*, directors can, in fact, be personally liable for not implementing a practice that would minimise harm to the company. It is not difficult to see how this could be applied in an AI context. As a result, directors should look to oversee that an appropriate AI governance framework is developed and implemented.

Effective AI governance begins with establishing the organisation's risk appetite for the use of AI. There is a delicate balance of moving swiftly but safely in relation to the adoption of AI. What's the company's appetite for risk when it comes to the use of AI, and what potential adverse consequences would the Board be willing to tolerate provided appropriate mitigations are in place?

Once this is defined, governance involves clearly defined internal organisational structures, roles and responsibilities, performance measures and accountability for AI outcomes that includes internal responsible stakeholders at a C-suite level.

A director's duty to act in good faith and for a proper purpose also extends to ensuring the AI governance framework considers the ethical implications of AI on the company. Adoption of AI must occur with an ethical mindset – consistent with the organisation's approach to business, its workforce, and data ethics.

There is a high use case for AI-augmented applications in workplace and workforce management. Not only is AI replacing certain roles in the business, but it is also making decisions about prospective workers and human capital management. Care must be taken by the company to ensure fairness, transparency and morality remain a stalwart to this use of AI – ethics will be critical in protecting the reputation and trust of any business moving forward.

The Australian Government Department of Industry, Science Energy and Resources has developed 8 voluntary ethics principles designed to build public trust in your company and positively influence outcomes from AI.[14] Implementing these principles into practice promotes fairness, protection, and security within your company is key to a director's duty in exercising their powers and perform their functions with care and diligence.

An example of some frameworks and guidance in relation to implementing AI governance can be found in the AIGA AI Governance Framework, PwC Responsible AI Framework and ISO/IEC 38507:2022 (further described on page 14).

The AIGA AI Governance Framework provides a template for directors and other decision-makers to ensure a practice-oriented framework for implementing responsible AI and adopting a systematic approach for AI governance.

05 Consider alignment with best practice AI risk management frameworks

Helpfully, there are a number of ethical AI and responsible AI risk frameworks/guidance published by both public and private sector entities (including the EU AI Act), which can form a useful base for any AI risk management framework.

These frameworks include:

- *ISO/IEC 23894:2023 - Information technology - Artificial intelligence - Guidance on risk management (further described on page 14)*
- *EU AI Act risk based regulation approach*
- *NIST Artificial Intelligence Risk Management Framework (AI RMF 1.0)*
- *US Department of Energy – AI Risk Management Playbook*
- *Microsoft Responsible AI Standards*

The NIST AI Risk Management Framework provides helpful direction and guidance to companies to improve its AI risk posture. It is designed to 'incorporate trustworthiness considerations into the design, development, use, and evaluation of AI products, services, and systems'.

The appropriate framework for your business will differ depending on your organisation's scope/use of AI tools and its risk appetite. The board should ensure that it is appropriately briefed by the business and subject matter experts in order to consider the appropriate framework to align the business against.

For further information on best practice risk management in the AI space, check out PwC's handbook on managing risk in the context of generative AI here.

14 Department of Industry, Science and Resources, Safe and responsible AI in Australia (Discussion Paper, June 2023)

ISO standards are already here…

The International Organisation for Standardisation has already developed key standards in relation to AI governance and risk management, which any director should be aware of:

ISO/IEC 38507:2022
Information technology - Governance of IT - Governance implications of the use of artificial intelligence by organisations

ISO/IEC 22989:2022
Information technology - Artificial intelligence - Artificial intelligence concepts and terminology

ISO/IEC 23894:2023
Information technology - Artificial intelligence - Guidance on risk management

Of particular importance is ISO/IEC 38507, which provides guidance to directors regarding the enablement and governance of AI, in order to ensure the development, deployment, and use of AI systems in the organisation is trustworthy, ethical, and transparent.

ISO/IEC 38507 – AI governance

The standard covers the governance and management of AI, including the development of relevant policies and procedures (eg on use of data, culture and values, decision-making involving AI), and how to manage key stakeholders.

Crucially, the standard reinforces the importance of human oversight and accountability in the use of AI systems. It establishes the need for clear risk management processes, focusing on accountability, reputation and trust, duty of care, safety, security and privacy of data/information for both current and future uses of AI.

The standard applies to all organisations, including public and private bodies, government entities, and not-for-profit organisations, of any size irrespective of their dependence on data or information technologies.

06 Embed ongoing assurance of AI

AI is not set and forget. The Court's expectations, as outlined in ASIC v RI Advice, is that there is very much an ongoing obligation to review and update the existing governance framework on a regular basis.

It is extremely important to set obligations around ongoing assurance, monitoring and testing of AI tools to ensure that they remain aligned with the organisation's business demands and obligations, as well as the requirement to meet changing technical specifications of AI and the needs of an evolving legal and regulatory landscape. Failure to do so may result in the degradation of AI model performance, also known as "drifting".

AI model drift occurs when the quality of the input data changes in a manner that lowers the accuracy of the AI prediction. In order to manage model drift, constant monitoring of the input data and the performance of the AI and its outputs is required. Directors must ensure there are suitably skilled company personnel checking data quality – where data quality has suffered, processes and procedures must be in place to retrain and fine tune the AI model to keep the model quality high.

Good governance practices spearheaded by the companies' directors and boards need to be agile. Appropriate care and diligence in discharging directors' duties calls for continued compliance with emerging legislation as it develops. Organisations should, therefore, implement routine health checks eg system reviews and auditing of data fed into AI models/systems to ensure it abides by all relevant privacy obligations and other local regulatory regimes.

Crucially, assurance in AI must be imported into every level of a business. There should be streamlined reporting from the operational functions to the board on AI implementation and use. Examples of such assurance reports would include (but not limited to) reports on any potential or current risks, user issues, security, and ethical concerns with AI.

Other considerations – can company directors use AI?

Robo-directors? AI in the boardroom

It almost makes sense for AI systems, with the ability to synthesise vast amounts of data in real time to conduct due diligence and respond to specific queries, to be used in the area of company decision-making. In fact, many companies have already done this – a Hong Kong firm relied on an AI bot to vote on an important financial investment decision for the company[15].

So why not let AI make all decisions for a director and replace the director? Firstly, the law has not yet moved to permit AI directors on boards. But it isn't impossible that this will be permitted (as seen above). In fact, as AI technologies become more prevalent and mainstream, directors may even be expected to use these tools in order to properly discharge their obligations.

However, at this stage, a director who determines that decision making can be resolved entirely by AI without themselves turning their mind to the decision and the surrounding information and facts, will likely expose themselves to liability for breach of their duties of care and diligence and, of independent judgment, by reason of reliance on or misuse of AI. Directors ultimately must "inform themselves about the subject matter of the judgement to the extent they believe to be reasonably appropriate" and then exercise that judgement.[16]

AI is simply a tool that directors may use to assist in their decision making and ultimately should not act in place of a director in its entirety and a director should always turn their mind to AI output before making a final decision.

ESG and AI

AI has a real potential to revolutionise our approach to major global challenges. Many companies have begun using AI to promote ESG practices, eg climate change modelling, fintech solutions to provide access to affordable financial services, energy management, etc. However, companies should also consider the potential ESG downsides of implementing AI to ensure that its use results in a net positive ESG outcome. For example:

- Lack of transparency in AI processes leads to inability to properly assess exact ESG impacts of AI-related investments. ESG-focused investors depend on the information that provided to ensure true change.
- In some circumstances, use of AI algorithms and data storage centres can increase the carbon footprint and energy consumption of a business. AI systems can require significant computing power to train large neural networks which may pose a threat to current ESG goals.
- As detailed earlier in this article, there is a real possibility of social discrimination and unethical outcomes in the implementation of AI models, if the right safeguards and controls are not in place for model design, model verification and ongoing model management.
- From a governance perspective, a key issue is a lack of technologically skilled staff from operational employees to those at the senior management level. As such, it is critical for directors and boards to upskill in AI, and ensure their organisation implements upskilling across the business.

15 BBC, *Algorithm appointed board director* (Web Page, 16 May 2014) <https://www.bbc.com/news/technology-27426942>.
16 *Corporations Act 2001* (Cth) s 180 (2).

Key Contacts

PwC's Digital, Cyber and Technology Law team, led by **Adrian Chotar**, is a team of specialist commercial, technology and intellectual property lawyers. We provide market leading solutions to help our clients solve their most complex information technology, data and legal problems.

Mainstream use of artificial intelligence (AI) exploded onto the scene with ChatGPT and given the myriad of commercial applications for generative AI, it is looking like it is very much here to stay. As a result, many agencies and businesses are looking to embed AI into their day-to-day operations. But in amongst the plethora of legal, commercial and risk issues related to AI, where do you start? How do you accelerate responsibly?

Please contact any of our team listed below to discuss how PwC can assist your organisation with your AI journey…

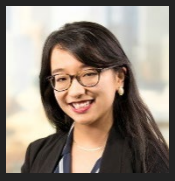
Adrian Chotar
Partner | Head of Digital, Cyber and Technology Law
PwC Australia
T: +61 (0)457 808 068
E: adrian.chotar@au.pwc.com

James Patto
Director | Digital, Cyber and Technology Law
PwC Australia
T: +61 (0)431 275 693
E: james.patto@au.pwc.com

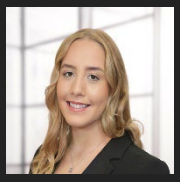
Mitchell Wright
Director | Digital, Cyber and Technology Law
PwC Australia
T: +61 (0)421 578 965
E: mitchell.wright@au.pwc.com

Authors and Contributors

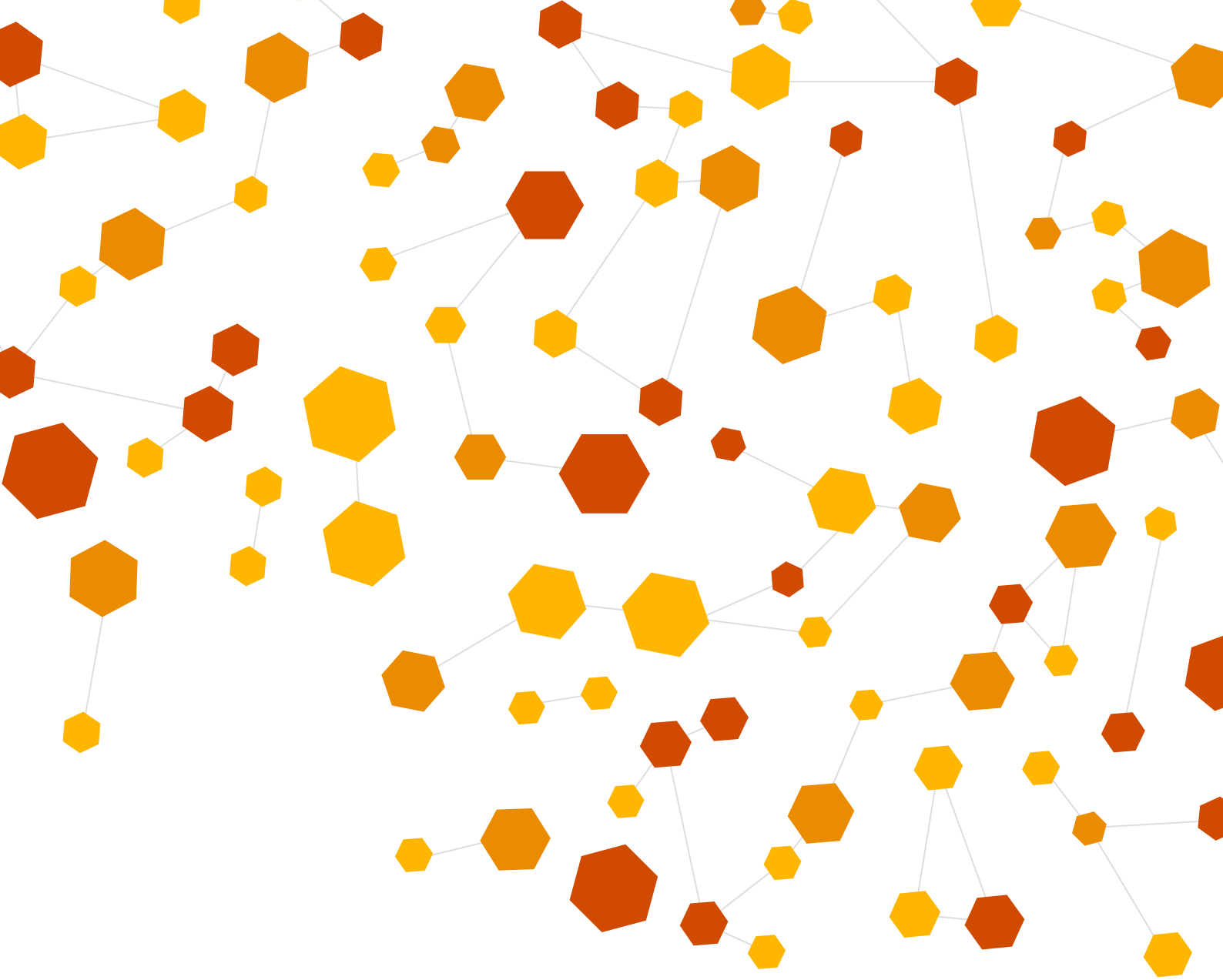
James Patto
Director | PwC Australia
Digital, Cyber & Technology Law



Annie Zhang
Associate | PwC Australia
Digital, Cyber & Technology Law



Gabrielle Knight
Graduate | PwC Australia
Digital, Cyber & Technology Law



A community of solvers coming together in unexpected ways to solve the world's important problems

www.pwc.com.au