SQUIRE
PATTON BOGGS

Local Connections. Global Influence.

AI and the Law in Australia and Abroad

A Risk and Regulatory Overview

Introduction

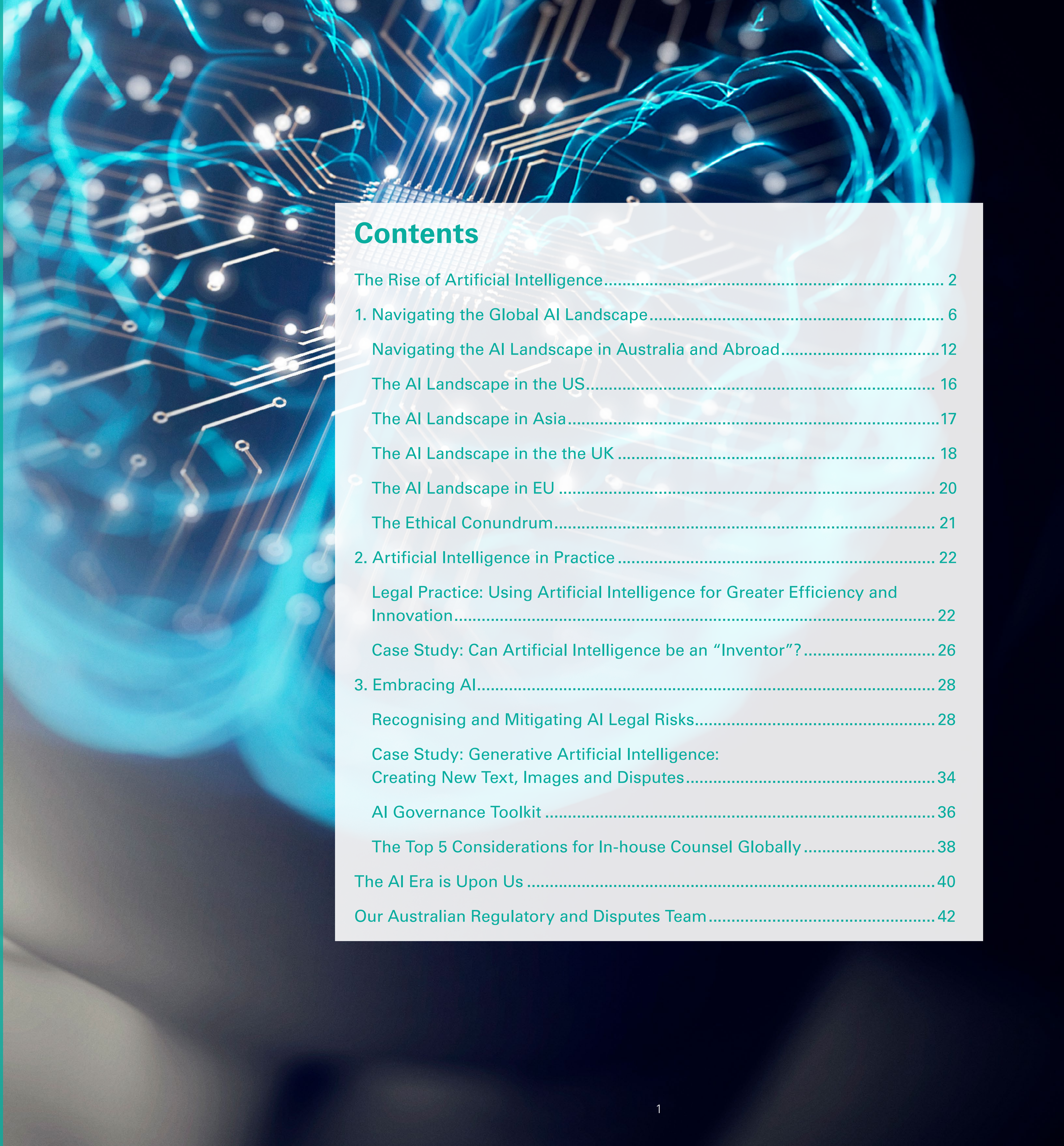
The scope and speed of developments in artificial intelligence (AI) have outpaced the expectations of many in industry and AI is now revolutionising thinking – not just in Australia, but around the world. AI is already having a significant impact on business, but it has become clear that we have yet to fully understand the potential applications, advantages and efficiencies.

Along with these applications, advantages and efficiencies come legal and other risks.

While different forms of AI have been around for some years, in 2023, it is generative AI that has really captured people's attention. As it does so, people are more closely considering both the benefits and risks of AI and, in particular, generative AI. Lawyers are central in the process of seeking to understand the risks and appropriately respond.

The legal risks, challenges and regulation of AI is where our firm can assist. We have extensive international expertise in the multifaceted commercial, contractual, data privacy, intellectual property (IP), regulatory, policy and other legal challenges that affect AI companies pushing the bounds of technology. With a diverse mix of capabilities and experience gained in the worlds of business, policy, law and technology, our multidisciplinary team has the resources, insight and business-minded, pragmatic skill sets to help our clients navigate the most pressing challenges and risks, make fast and effective decisions, build new business models and, most importantly, thrive.

Please note that the information in this document does not constitute legal advice. For legal guidance, please contact one of our legal experts, whose contact details can be found on p 43.



Contents

The Rise of Artificial Intelligence

Artificial intelligence (AI) refers to the interaction of various technologies, working together to enable machines to learn, understand, predict and, in part, simulate human cognitive processes.

When AI technologies are used in combination with data and automation, they can enable the adopter to work more efficiently in achieving their tasks and objectives.[1]

The interest in, and anticipation around, AI has been building for quite some time. This has largely been driven by the masses of data that we produce each day through our day-to-day activities and interactions, as well as developments in data centres, like the Cloud. Although we are in the early stages of the AI era, interest and adoption is accelerating at a rapid pace, with huge investments being made by all the big tech players, including Microsoft, Google, Amazon, Meta and IBM.[2]

Today, AI exists in a multitude of formats, and in some areas has become a staple in our everyday lives. Take Google, for example, which uses big data analytics to search the web for patterns, trends and information that will provide us with the answers to our questions. Anyone who uses virtual assistants such as Siri or Alexa engages with a form of AI called natural language processing, in which computers combine the identification of spoken word with learned context to understand our instructions. We would be remiss to not mention the infamous rise of ChatGPT – the latest generative AI model that was smart enough to pass the US bar exam earlier this year, forcing legal professionals around the world to take notice.

[1] Accenture.com/insights/artificialintelligence.

[2] Thomson Reuters, "Australia: State of the Legal Market Report – Navigating towards prosperity amid challenges".

Artificial Intelligence and the Legal Profession

AI appears to have an important place in the legal profession.

Current trends show that larger law firms are ahead in the use of, or the desire to use AI, demonstrating a greater willingness to accept the risks for the potential rewards. Meanwhile, mid-size and smaller firms, as well as in-house legal teams, seem to generally be taking a more cautious approach.[3] Nevertheless, investment in technology by law firms continues to increase, where firms are utilising technology to address challenges relating to utilisation, rising costs and talent retention, while simultaneously delivering a digital transformation of the business.[4]

The different types of AI promise to enable lawyers to deliver a faster service, with more thorough advice and creative solutions, and to strengthen their client relationships. However, the true impact of AI needs to be carefully considered and assessed, and will likely differ across practice areas, firms and clients.

As AI use increases in law firms, legal teams are likely to require more AI-trained lawyers to service clients. This creates training opportunities for existing employees, and the concept of working with new, novel AI capabilities is going to be an attractive feat when recruiting new talent. Generative AI, if used correctly, could also enable lawyers to spend less time on repetitive, manual processes and more time on meaningful, value-added tasks, which may lead to improved employee satisfaction, and help to retain talent. However, along with the changes in legal practice, training, and potential efficiencies comes the risk of redundancies.

Simultaneously, AI has the potential to impact the needs that internal counsel have for assistance from external counsel. In-house counsel are likely to expect enhanced transparency and understanding of the extent of AI involvement in the services they receive and may seek cost savings if AI is used. Furthermore, it increases their buying power and creates a more competitive environment in which external counsel will need to compete for work.[5]

[3] Thomson Reuters, "Australia: State of the Legal Market Report – Navigating towards prosperity amid challenges".

[4] Thomson Reuters, "Australia: State of the Legal Market Report – Navigating towards prosperity amid challenges".

[5] Thomson Reuters, "Australia: State of the Legal Market Report – Navigating towards prosperity amid challenges".

Artificial Intelligence and the Competitive Advantage

A technologically enabled business, regardless of sector, promises to have a level of competitive advantage.

These advantages include potential cost reductions, workflow efficiencies and improved accuracy in decision-making, and AI has the potential to further expand these benefits in legal practice. Furthermore, AI could be used to support businesses in achieving their environmental, social and governance (ESG), and diversity, equity and inclusion (DEI) objectives, further strengthening their competitive advantage in the market.

While AI has been used for some time, the pace of change has increased significantly in the last year. With this acceleration, there are practical, regulatory and ethical considerations, and these factors result in understandable caution in embracing AI in business.

Advantages of Artificial Intelligence

- AI can assist with the digital transformation of a business.
- The novelty and enhanced job satisfaction that comes from working with AI may attract new talent, as well as retaining existing talent.
- AI can provide cost-reduction benefits where alternative resources are more effectively utilised.
- AI can improve workflow efficiency by automating time-consuming processes, which, in turn, creates capacity for more meaningful, strategic tasks.
- AI has the potential to deliver improved accuracy and decision-making, which, in turn, provides an enhanced quality of output and reduces the risk of error.
- Where AI thinks differently from humans, it could offer alternative insights and support business innovation in a way that may not be possible in human capacity.
- AI, when used appropriately, promises to enable the provision of all-round improved client service, which, in turn, will strengthen client relationships.
- AI can be used to support businesses in achieving their ESG and DEI objectives through improved benchmarking, reporting mechanisms and verification.

Disadvantages of Artificial Intelligence

- The implementation of AI poses a threat to jobs where its cost-effective and efficient nature will likely lead to either a change in job requirements or redundancy for many traditional roles.
- At present, in the early stages of AI adoption, there is a lack of integration between technology platforms and various overcomplicated systems/processes, which pose both knowledge and technical obstacles.
- The regulatory landscape is still developing, and this poses both uncertainty and risk to businesses. Regulatory approaches vary from country to country.
- There is a lack of education programmes and resources to support businesses with understanding the legal risks that AI poses to their business.
- AI creates potential liabilities in the form of:
  - Misinformation (including defamation)
  - Bias and unlawful discrimination
  - IP infringement
  - Data privacy and confidentiality breaches, as well as cybersecurity breaches, including fraudulent or other illegal activity

Navigating the AI Landscape

The opportunities presented by technological change also come with several risks and an evolving regulatory landscape.

In Australia, we do not have specific regulations or laws that deal directly with AI. Instead, AI is currently regulated through existing laws (for example, concepts of administrative law, and laws relating to consumer protection, intellectual property and discrimination) as well as a voluntary ethical framework. However, with the upsurge in AI interest and adoption in 2023, there appears to be a growing appetite for more specific regulatory reform.

At present, it is unclear what this reform will look like. On 1 June 2023, the Australian government released a discussion paper, "Safe and Responsible AI in Australia", which sought feedback from industry on the development of a new regulatory framework. At the time of writing, the outcome of this discussion paper is yet to be revealed. However, future regulatory frameworks are predicted to be based on the EU AI Act and Canada's Artificial Intelligence and Data Act (AIDA), which are considered to be two of the most advanced and comprehensive frameworks in existence, and appear to have set the precedent for any future regulation.

Generative AI poses a threat to data privacy and cybersecurity (DP&C). Both of these are already a key concern for businesses. The Australian Securities and Investment Commission (ASIC) continues to focus on managing cybersecurity risks and enhancing resilience to cyberattacks, as well as enforcing action against organisations for governance failures relating to cyber resilience and failure to mitigate the risk of cyberattacks.

Additional risk lies in misinformation produced by generative AI tools and subsequent consequences for how that information is used. Additionally, potential risks can be seen in areas such as defamation, where false information might be relied upon, resulting in defamatory imputations. Similarly, there is risk that content produced by generative technologies will infringe on existing copyrights or trademarks. The output of generative AI comes from the data it is fed and, as a result, this output may well be taken without permission from a work that is protected. Even where new work is created, there is an ongoing discussion around who owns the IP in relation to the content produced by AI.

The Future of AI

Today, more and more business leaders recognise that AI has the potential to transform their business and the market in which they operate. Some are well on their way to embracing the change, and others still have a long way to go.

Interest and attitude to experimentation among businesses appears to be growing very quickly, and a moderate increase in tech-based investment in the coming months has been predicted.[6] However, there is still so much uncertainty around the future of AI and with little guidance around how to navigate the challenges that lie ahead, it is only natural for businesses to be cautious in their adoption.

Our report, "AI and the Law – A Risk and Regulatory Approach", intends to help businesses on their journey of understanding the current position and future of AI from a legal perspective. In the pages that follow, we provide a comprehensive overview of the regulatory landscape in different jurisdictions, identify some of the risks associated with AI, and provide practical guidance on how to mitigate these risks and to successfully implement AI into your business.

[6] Thomson Reuters, "Australia: State of the Legal Market Report – Navigating towards prosperity amid challenges".

1. Navigating the Global AI Landscape

Australia

Along with the rest of the Asia Pacific region, there is an absence of AI-specific regulation in Australia. Existing policy is focused on remaining technologically neutral to prevent being left behind as technology advances.

In place of a direct regulatory approach, the AU government was one of the first governments in the world to produce AI ethics principles that align with the international standards set out by the Organisation for Economic Development (OECD).

The AI ethics framework is voluntary, but the following are not:

Privacy Act
Online Safety Act
Australian Consumer Law
Administrative law concepts
Intellectual property laws
Anti-discrimination laws

New Zealand

The primary legislative framework for AI in New Zealand is the Privacy Act (2020), which establishes how personal data can be collected, processed and used.

At present, New Zealand does not have an AI strategy, or any plans to develop specific AI regulation. However, it has:

- Adopted the OECD Principles on Artificial Intelligence relating to public policy and strategy recommendations to ensure ethical and responsible use of AI
- Created a tool for government agencies to use when assessing the ethical and legal implications of using AI in decision-making processes – this is known as the Algorithm Charter for Aotearoa New Zealand
- Developed a roadmap for the regulation of AI in partnership with the World Economic Forum's Centre for the Fourth Industrial Revolution
- Signed the Digital Economy Partnership Agreement with Singapore and Chile, which establishes new rules and guidance on digital trade and emerging issues, including AI

Canada

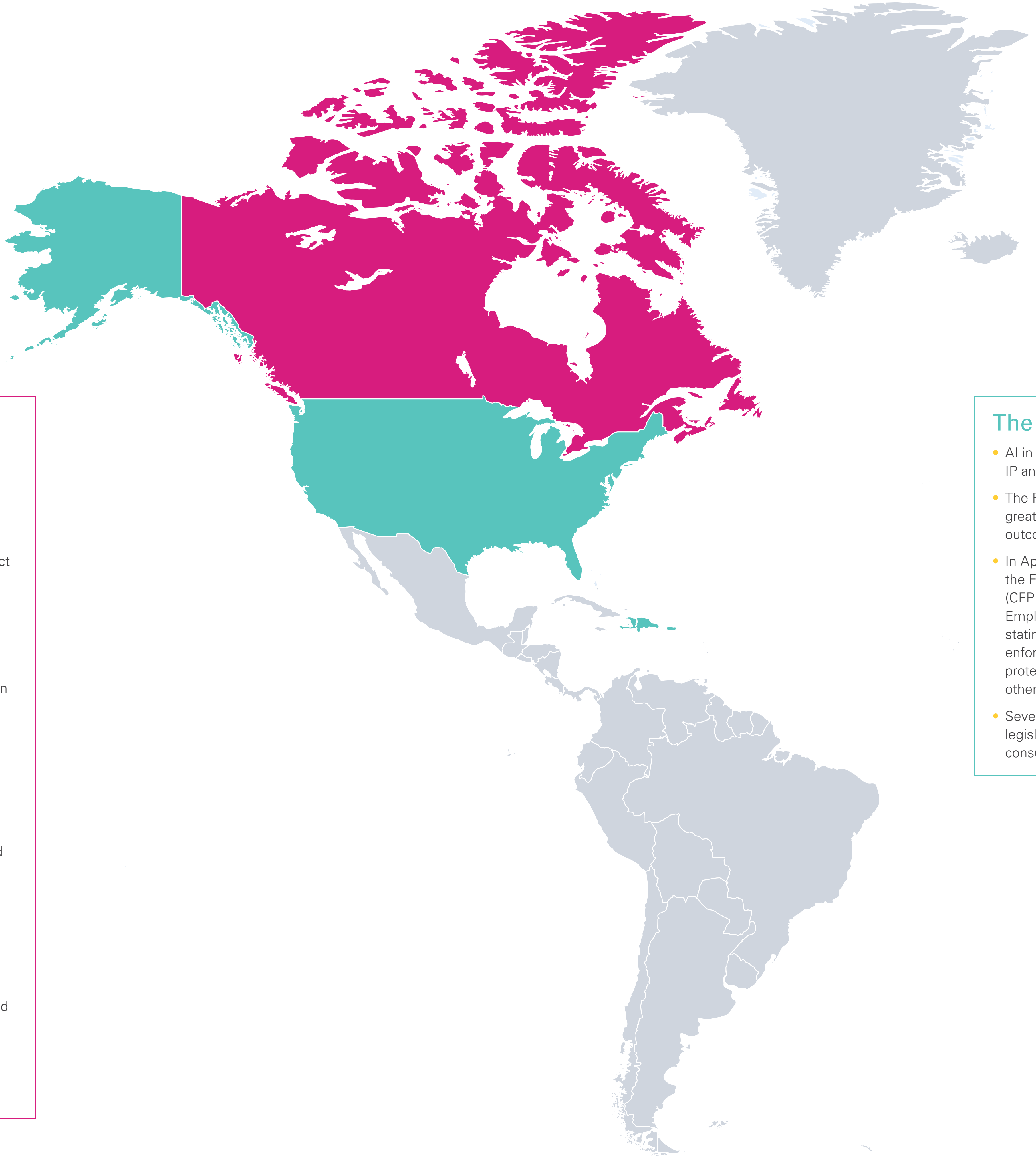
The proposed Artificial Intelligence and Data Act adopts a principles-based approach and intends to mitigate the risk of bias and harm caused by AI in a manner that also allows for technological innovation.

The Artificial Intelligence and Data Act (AIDA):

- Imposes transparency requirements on high-impact systems and does not ban systems presenting an unacceptable level of risk
- Has limited application by the constraints of the federal governments' jurisdiction
- Only imposes data governance requirements on the use of anonymised data, but this will develop in future regulation
- Requires responsible persons to implement mitigation, monitoring and transparency measures and comply with record-keeping requirements
- Specifies a penalty of up to CA$25 million or 5% of the offender's gross global revenues from the preceding financial year, as well as new criminal offences for the most serious offences committed under the act

In September 2023, the Canadian Minister of Innovation, Science and Industry announced the Voluntary Code of Conduct on the Responsible Development and Management of AI Systems. The code temporarily provides Canadian companies with common standards and enables them to demonstrate, voluntarily, that they are developing and using generative AI systems responsibly until formal regulation is in effect.[1]

[1] https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act.



The US

- AI in the US is currently regulated by existing privacy, IP and employment laws, to name just a few.
- The Federal Trade Commission (FTC) has signalled greater scrutiny is coming in relation to the fair outcomes of AI and false claims made by AI.
- In April 2023, a joint statement was made by the FTC, Consumer Financial Protection Bureau (CFPB), Department of Justice (DOJ) and Equal Employment Opportunity Commission (EEOC), stating that each agency will be using its respective enforcement powers to regulate the use of AI to protect consumers from discrimination, bias and other harms.
- Several states have already introduced AI-specific legislation in the last several years and new state consumer privacy laws regulate some types of AI.

The UK

- The current UK government does not plan to enact new laws or regulations aimed at governing AI – rather existing laws and regulations will continue to apply, and be enforced by the existing regulators, on the use of AI, rather than the AI technology itself.[1]
- The UK has established a government-industry taskforce, called the Foundation Model Taskforce, to engage with generative AI developers in establishing safety and security standards.[2]
- The UK has indicated a pro-innovation approach to AI, with its whitepaper – published in March 2023 – showcasing the core principles for the regulators to abide by when constructing a non-statutory AI framework. These principles relate to safety and security, transparency, fairness, accountability and governance.[3]

[1] https://www.rpc.co.uk/perspectives/tech/the-unicorn-kingdoms-ai-white-paper/.

[2] https://www.gov.uk/government/news/initial-100-million-for-expert-taskforce-to-help-uk-build-and-adopt-next-generation-of-safe-ai.

[3] https://www.lexology.com/library/detail.aspx?g=a8f0fc00-52f4-4562-a82f-bf45b665ccf9.

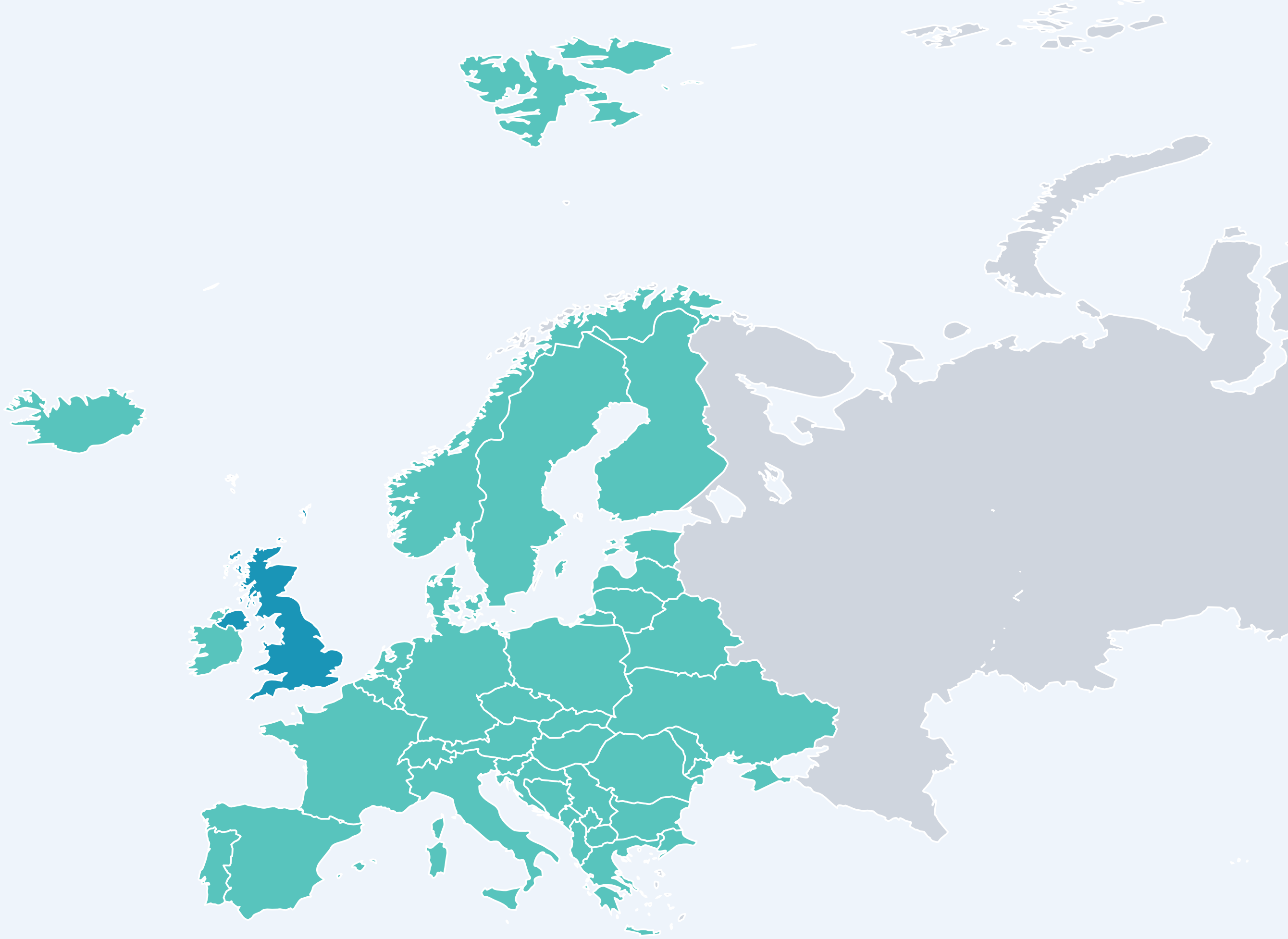
Europe

The EU Artificial Intelligence Act (EU AI Act) was one of the first attempts, globally, to create a comprehensive regulatory framework for AI. It is not yet adopted but should be soon.

The EU AI Act:

- Specifies a list of prohibited uses of AI (such as for social scoring).
- Permits the use of high-risk systems (including facial recognition by private actors) but mandates, among others, thorough testing, evidence of quality data and an accountability framework.
- Specifies a penalty of up to €30 million or 6% of gross global revenues from the preceding financial year for non-compliance with prohibited AI practices or the quality requirements set out for high-risk AI systems. There are discussions for those fines to be even higher.
- Specifies the enforcement framework that will be left to member states, even if a form of consistency should come from an AI board, the latest addition to the list of EU institutions.

If the EU AI Act passes into law in its current form, then it will be one of the strictest approaches to regulating AI seen globally thus far. Until then, the EU supervisory authorities continue to scrutinise AI through other lenses, data protection laws being an important one.



Japan

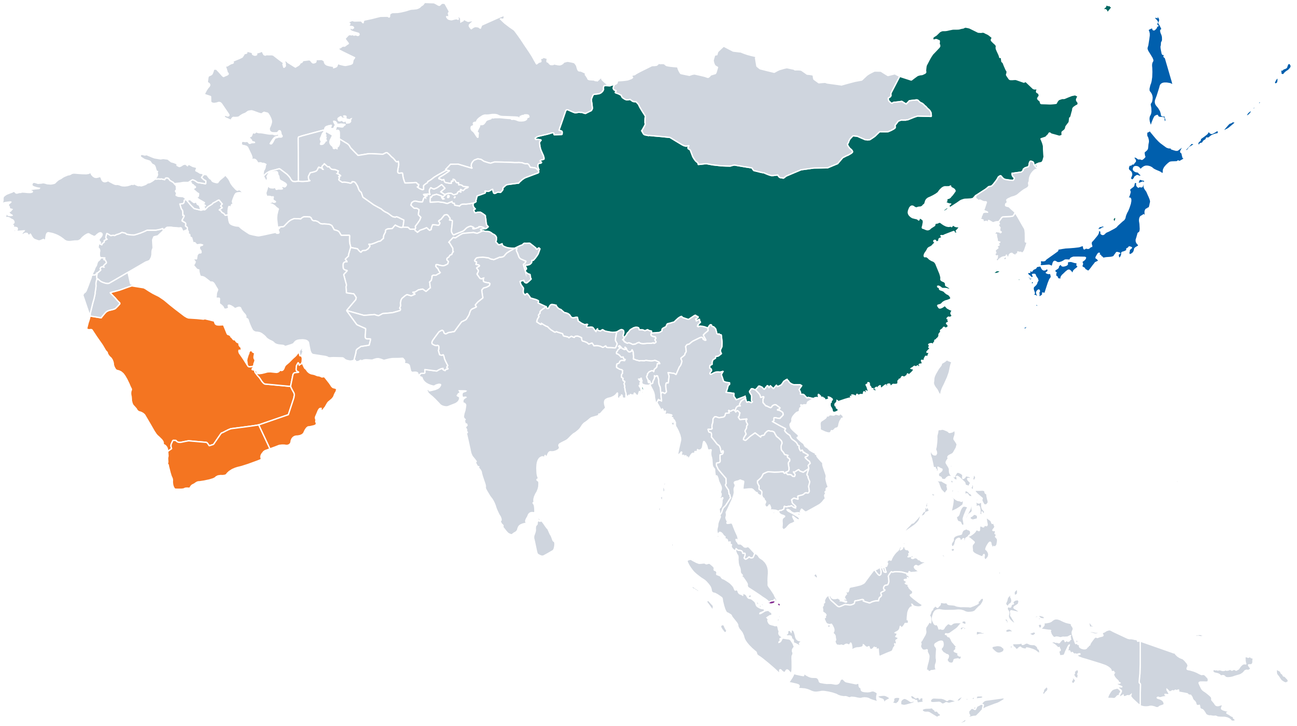
There is currently no AI-specific legislation or regulation of AI. Instead:

- There is guidance in the form of the Provisional Summary of Issues concerning AI (23 May 2023)
- Existing guidance has a focus on addressing privacy risks and is enforced by the Personal Information Protection Commission (PIPC)
- The use of AI in conducting crimes is governed under the Penal Code and the Consumer Act, which also seeks to address the risk of fake news, created by generative AI

China

China Interim measures for the management of generative AI services (2023).

- These measures apply to AI services that are provided to the public (rather than B2B) and are enforced by the Cyberspace Administration of China (CAC). The measures also apply extraterritorially, and although the CAC cannot enforce its powers outside of China, it can notify local regulatory bodies where foreign businesses are providing AI services to the general public of China.
- To operate generative AI, an ICP licence is required, and businesses may be subject to other licencing requirements dependent on their sector, e.g., press and publication sectors, and TV and film sectors.



Middle East

At present, there is no overarching framework for the Middle East region, and most countries regulate AI through existing laws such as data protection, IP, product safety, consumer protection legislation, medical device regulation, financial services regulation and cybersecurity laws.

Most countries in the region understand the importance of ethics in relation to AI and have included ethical components in relation to their strategic AI visions.

Singapore

Has established an advisory council on ethical use of AI and data, as well as developing a Model for AI governance framework and an implementation and self-assessment guide.

Additional guidance includes:

- AI Verify – an AI governance testing framework and toolkit
- Veritas open-source toolkit
- AI in healthcare guidelines

Navigating the AI Landscape in Australia and Abroad

AI has the potential to benefit society in ways that we likely do not or cannot currently comprehend.

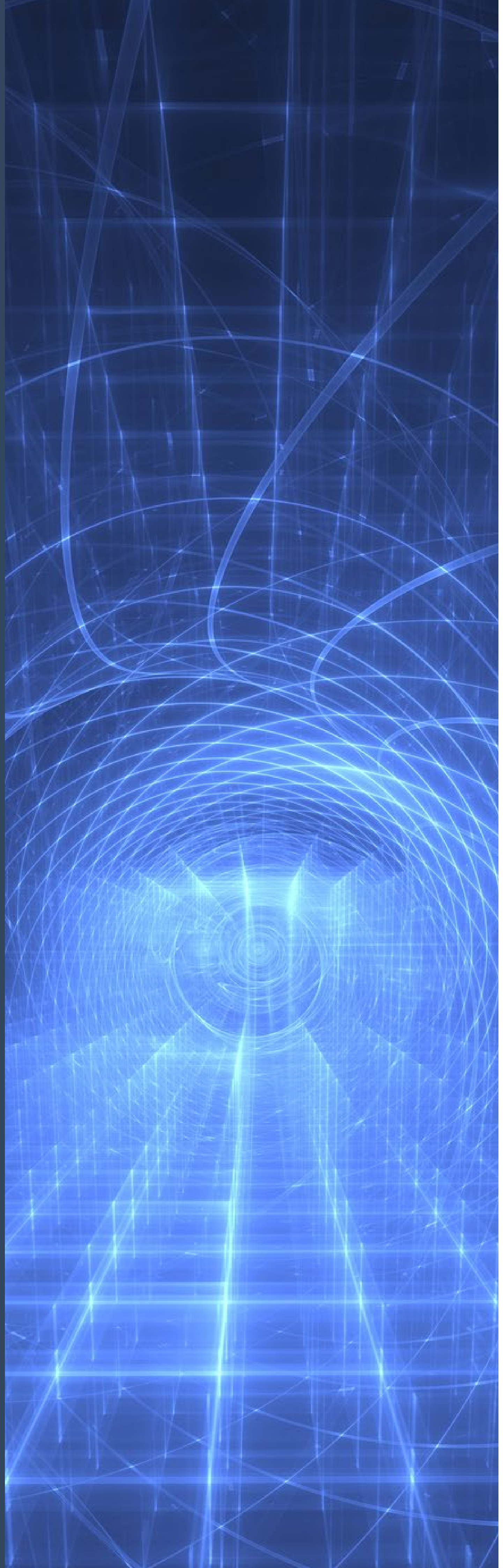
AI's potential for autonomy and recursive self-improvement gives rise to a question as to how safe we really are from the risks of AI, and how the government will seek to regulate these advances in technology to ensure that AI does not encroach our fundamental rights.

Fiction is replete with dystopian portrayals of an intelligent machine turning on its former master. Stanley Kubrick's 1968 classic *A Space Odyssey* features HAL-9000, an artificially intelligent onboard computer that malfunctions and turns on the crew. James Cameron's *Terminator* involves an artificially intelligent defence system, Skynet, achieving self-awareness and embarking on the extermination of the human species. In reality, of course, the perils of AI and the attendant challenges of regulating it are far more nuanced.

Assuming that we can avoid total annihilation, AI technologies create risks in fields as disparate as privacy, defamation, discrimination, IP, copyright, consumer protection, administrative law, criminal liability and ethics. Australia is not alone in assessing the most appropriate framework to regulate AI and, as one of the first countries to adopt a national set of AI Ethics Principles, can consider itself an early mover on responsible AI.

Nevertheless, there remains work to be done, and the international approach to AI regulation is far from uniform. As can be seen in the summary of the different global laws in the section of this report titled "Navigating the Global AI Landscape", some countries have embraced the idea of the sufficiency of voluntary mechanisms in the form of ethical guidelines and standards. In other jurisdictions, the imposition of formal, AI-specific legal obligations are preferred. Australia finds itself at a crossroads in the search for an appropriate balance between the promotion of innovation and the myriad of regulatory challenges posed by AI. As with any legislative reform, much can be gained from attention to the initiatives and experiences of other legal systems.

This article, and the global insights that follow, provides an overview of the current AI regulatory landscape in Australia, where things might be heading and what can be learned from abroad.



The AI Regulatory Landscape in Australia

To date, the Australian government's response to emerging AI technologies has not extended to AI-specific regulation. Instead, the government has relied upon the applicability of several existing laws and implemented voluntary frameworks such as the AI Ethics Principles, released by the Commonwealth Department of Industry, Science and Resources (DISR) in 2019.

The AI Ethics Principles are based on the Organisation for Economic Co-operation and Development's (OECD) Principles on AI (now adopted by over 40 countries) and focus on concepts like human, societal and environmental wellbeing, human-centred values, fairness, privacy, reliability and safety, transparency, explainability, contestability and accountability. The AI Ethics Principles are not binding and the DISR concedes they are aspirational and intended to complement and not act as a substitute for an appropriate regulatory regime.[7]

Similarly, the Australian Digital Transformation Agency (DTA) has provided a guidance paper on the adoption of AI by the public sector. The National AI Centre, coordinated by CSIRO, has also established a Responsible AI Network (RAIN) that aims to provide Australin businesses with best practice guidance, tools and learning models guided by world-leading experts. While these resources are of utility to the Australian business community, they are carrots in a world that requires sticks.

As noted above, beyond the voluntary framework, the regulation of AI technology in Australia relies on a spectrum of existing laws of broad application. They may be of a general nature, for example the Australian consumer law, competition laws and human-rights based discrimination laws, or sector-specific legislation, for example regulatory regimes relating to therapeutic goods, motor vehicles, airline safety or financial products. The salient question is whether these laws, drafted to prohibit or remedy a specific mischief without regard to any AI-associated risk, are fit for purpose in this brave new world of rapidly developing AI technology.

In this context, in June 2023, DISR released a discussion paper entitled "Safe and Responsible AI in Australia".[8] Over 448 public submissions were received in response to the discussion paper. From those submissions, broadly speaking, three reoccurring themes emerge:

- First, the suitability of the existing technology-neutral legislation can only be answered after a comprehensive review of relevant Commonwealth and State laws to truly understand if AI-specific legislation is necessary. A cautious and methodical approach is appropriate, and the Australian government should avoid rapid implementation of AI-specific laws as a reaction to the significant media attention created by the release of new generative AI platforms and the corporate stampede to capitalise on those technologies. Such a rapidly introduced regime might create conflicts and inconsistencies with existing laws and through this or separately lead to unintended outcomes. It could be that AI-specific regulation need only focus on the specific risks posed by AI that simply cannot be addressed by existing laws, such as the prohibition of red-flag high-risk AI systems, mandatory transparency requirements for AI developers and surveillance issues.
- Second, irrespective of the need for AI-specific legislation, it is necessary to consider whether the existing regulatory regimes of broad application are appropriate and adaptable to AI risks. There are numerous situations in which it remains unclear if existing prohibitions would capture AI cases or whether loopholes need to be addressed. Some limited examples include:
    - The extent to which prohibitions on misleading or deceptive conduct will apply to AI generated material[9]
    - Whether an AI system that sets prices by reference to the market might result in a substantial lessoning of competition[10]
    - Whether certain AI solutions might be considered services as opposed to goods for the purpose of the Australian consumer law and, therefore, be immune to the product liability regime.
    - How IP rights can be infringed by AI-generated materials
- Third, if AI-specific legislation is to be introduced, should it adopt a principles-based approach comparable with the Australian Privacy Principles, and should the new legislation be administered by a new regulator, or an existing regulator with an expanded remit? The submissions also frequently suggest that any AI-specific regulation in Australia should look to the steps being taken abroad and adopt a consistent and commensurate approach.

This last proposal is undeniably sensible, although the fundamentally different approaches being adopted by other jurisdictions indicates that there is no single fix or universally accepted school of thought when it comes to AI regulation.

[7] https://www.industry.gov.au/publications/australias-artificial-intelligence-ethics-framework/australias-ai-ethics-principles.

[8] https://consult.industry.gov.au/supporting-responsible-ai.

[9] Competition and Consumer Act 2010 (Cth), Sch 2, section 18.

[10] Ibid, section 50.

The Approach to AI Regulation Abroad

To date, the EU's Artificial Intelligence Act (EU AI Act) and Canada's Artificial Intelligence and Data Act (AIDA) are considered two of the most advanced and comprehensive frameworks in development, providing a framework for the development of regulation across the globe.

The EU

The European Union (EU) has undertaken significant work in the area of AI. In 2021, the EU tabled an ambitious regulatory framework (the EU AI Act) which is currently being negotiated in a trilogue between EU member states on the Council. European Commission and European Parliament: the aim is to reach an agreement by the end of 2023. Once the terms are finalised, there is likely to be a two-year grace period for implementation and adoption. The EU AI Act adopts a 'risks based' approach to regulation, classifying AI systems as unacceptable risk, high risk, limited risk, or low risk.

In the first category classified as unacceptable risk, AI systems such as cognitive behavioural manipulation of persons, 'social scoring' (the classification of persons based on behaviour, socio-economic status or personal characteristics) and 'real time' biometric identification systems will be prohibited. The explanatory materials to the EU AI Act indicate that some exceptions may be allowed, for example biometric identification systems where identification occurs after a significant delay to prosecute serious crimes, but only after court approval.

AI systems classified as 'high risk' are those which may negatively affect safety or fundamental rights. These include systems used in products falling under EU safety legislation (toys, aviation, cars, medical devices, lifts etc) and systems used in education and vocational training, employment and worker management, access to public services, law enforcement and migration and asylum. High risk AI systems will need to be assessed before entering the market and will need to be registered on an EU AI database.

Generative AI, like ChatGPT, will need to comply with certain transparency requirements such as disclosing that content was generated by AI or that AI designed the systems, so they do not generate illegal content. Limited risk systems such as systems that generate or manipulate images, audio or video content will need to comply with some minimal transparency requirements, for example informing users that they are interacting with an AI system, and it is likely that AI companies will be encouraged to voluntarily sign up to codes of conduct which mandate similar requirements to high-risk AI systems.

Canada

In September 2023, the Canadian Minister of Innovation, Science and Industry announced the Voluntary Code of Conduct on the Responsible Development and Management of AI Systems. The code temporarily provides Canadian companies with common standards and enables them to demonstrate, voluntarily, that they are developing and using generative AI systems responsibly until formal regulation is in effect.[11]

In the meantime, the Canadian parliament is considering the terms of the AIDA that would set the foundation for the responsible design, development and deployment of AI systems in Canada and ensure that they are safe and non-discriminatory.[12] The proposed legislation sets out a risk-based approach to regulating AI systems and will hold companies responsible for the AI activities under their control. Companies will be required to provide an account of their use of automated decision-making systems to make predictions, recommendations and decisions, and to provide an explanation of how the prediction or decision was obtained when that information is requested by the individual affected.[13]

Businesses will also be required to assess the intended uses and limitations of their AI systems, put in place appropriate risk mitigation strategies and ensure their AI systems are continuously monitored.[14] Following the introduction of the legislation, the Canadian government is intending to conduct a broad and inclusive consultation of industry, academia and the Canadian public to inform the implementation of the regime.[15]

[11] https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act.

[12] Ibid.

[13] Parliament of Canada, Bill C-27, Government of Canada, 22 November 2021.

[14] Ibid.

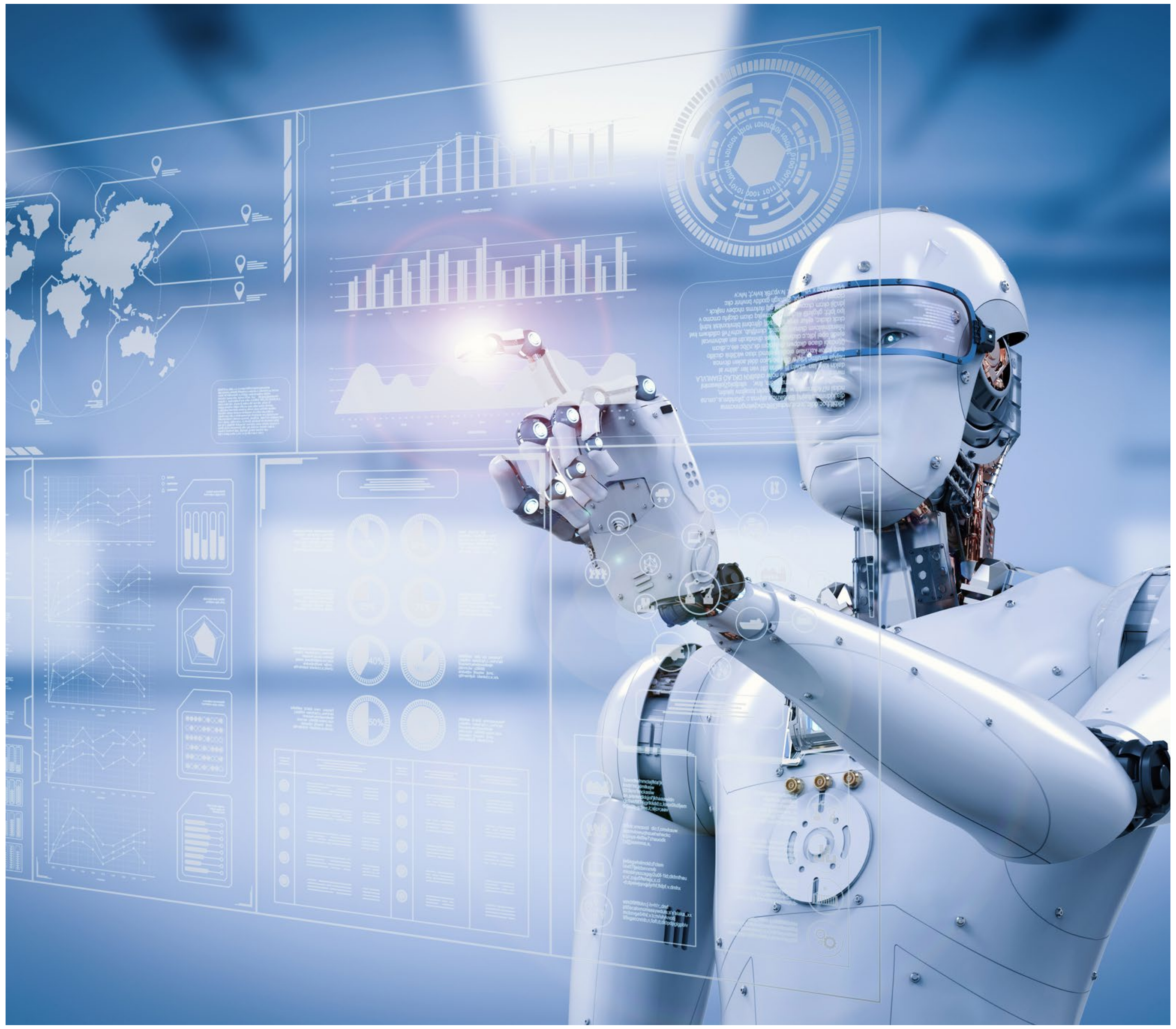
[15] See: https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document#s10.

Where Next for Australia?

Considering the submissions made to DISR's Safe and Responsible AI in Australia working paper, if those views are taken onboard, the next step for Australia may be a root and branch review of how effective the existing regulatory regimes of general application are to addressing specific AI-related risks. It is likely that some reform will be recommended.

As DISR notes in the working paper, it is essential to avoid a piecemeal regulatory environment that may act as a barrier to industries adopting productivity enhancing AI technologies in Australia. Equally important is that Australia's governance framework is harmonised with those used globally, including its major trading partners, to ensure Australia is positioned to take advantage of AI-enabled systems that are supplied on a global scale.

The real balancing act is ensuring that there are appropriate safeguards for high-risk AI systems without restricting innovation and allowing Australian businesses to confidentially develop and invest in AI systems with clarity in relation to the associated obligations and restrictions. It may be inevitable that some additional legislation is required to regulate red-flag high-risk AI systems, transparency requirements for AI developers and certain surveillance issues associated with the AI. Whether that is best achieved with a risks-based regime like the EU AI Act and Canada's AIDA or, as an alternative, a more flexible proportionate, pro-innovation approach remains to be seen. Time will tell.



The AI Landscape in the US

C-suite executives, boardroom directors, legal departments and policymakers are evaluating what AI could mean for their companies, capital markets, the economy and general society. While AI promises innovation, enhanced efficiencies and cost reductions, there are also concerns about risks to the workforce, consumer privacy, IP rights and discrimination, to name just a few. As a result, policymakers are constructing a regulatory framework that addresses a broad range of concerns, but at the same time remains flexible and relevant as AI continues to evolve. Companies are developing responsible AI use policies and training personnel on how and when to use AI, balancing risk and reward.

As AI evolves, its impact will span many aspects of society, and the issues that it presents are varied. In turn, a range of legislative committees and regulators are involved in this debate. An added complexity is that a handful of individual states have already implemented AI-specific legislation and new consumer privacy laws, which are creating a patchwork of regulation and requirements for businesses to navigate when operating in the US.

At present, AI at the national level is governed by a set of existing laws, including privacy, IP and employment laws, to name just a few. However, the Federal Trade Commission (FTC) has signalled that greater scrutiny is coming in relation to fair outcomes of AI and false claims made by AI. Furthermore, in April 2023, a joint statement was made by the FTC, Consumer Financial Protection Bureau (CFPB), Department of Justice (DOJ) and Equal Employment Opportunity Commission (EEOC), stating that each agency will be using their respective enforcement powers to regulate the use of AI to protect consumers from harm.

So far, the debate around AI has drawn out eight key concerns that are top of mind for both businesses and policymakers. These include national security, data privacy, bias and discrimination, accountability, transparency, copyright, the workforce and deepfakes. The US government's National Institute of Standards and Technology (NIST) has developed an AI Risk Management Framework and related guidance materials to help companies address these concerns in a responsible manner.

As the debate around AI regulation continues to evolve, we expect to see a federal legislative framework that is less prescriptive than the EU AI Act and Canada's AIDA and more reflective of the NIST approach. However, state and even local laws could be passed that are more cumbersome, such as a recently passed ordinance in New York City that tightly regulates use of AI in the human resources context.

AI presents a significant competitive advantage to businesses; however, the associated reputational and liability risks are prevalent.

Alan Friel
Global Chair, Data Privacy, Cybersecurity & Digital Assets,
Los Angeles

The AI Landscape in Asia

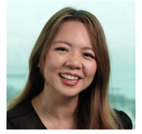
There is no region less monolithic – or more diverse – than Asia, not only when looking at the maturity of technical infrastructure needed for AI development, but also at the policy objectives around and consequential pace of regulation for AI use.

Yet the region is extremely significant, not least because of its staggering population, which, in aggregate, dwarves the rest of the world's. India, China and Indonesia, in particular, are the most, second most and fourth most populous nations in the world, respectively. As such, when discussing the impact that AI will have on this region, it is easy to see this watershed time can only magnify existing disparities among Asia Pacific states. In jurisdictions that are high-tech and hyper-connected – South Korea, Japan and Singapore, for instance – there are already established laws in place on the use and deployment of AI products and systems. These span, non-exhaustively, contract, IP, product safety, consumer protection, data privacy, cybersecurity, antitrust and competition, content moderation and info-communications licensing. In contrast, "emerging markets", especially in Southeast Asia, have much less in terms of legislation that apply to technology, data and AI.

In view of all this, it would be somewhat challenging to try to reach any form of an Asia-wide consensus with regard to addressing AI-risks and harnessing its tremendous potential and associated opportunities. As to whether this can ultimately be achieved will likely depend on whether governments in Asia are first and foremost willing to adopt common principles, or even to model their respective approaches to AI governance on the EU AI Act, similar to how many Asia Pacific jurisdictions have passed (or are looking to pass) data and privacy laws modelled after or upon the EU GDPR. Examples are Thailand, India, the Philippines and even China.

Also, while many nations across Asia Pacific have adopted or endorsed some form of an AI strategy or agenda, only a handful are gearing up towards enacting standalone AI legislation. These include South Korea, Thailand and China, which we detail further below. Others like Singapore and Japan, on the other hand, seem more inclined to building on existing frameworks (perhaps adopting modifications as appropriate), rather than prematurely or over-regulating AI.

- In August 2023, China implemented what some have observed to be one of the most far-reaching and restrictive generative AI measures around the globe. It applies to the provision of generative AI to the public (as opposed to B2B), and some of its unique features include not doing anything to undermine China's socialist core values. Further, to the extent that the AI system generates any text, pictures or videos, these will likely be subject to government pre-approval, as well as the need for other government licences as may be further specified. This would make it highly unlikely for any foreign generative AI provider to be able to launch a public service in China.
- In South Korea, the (Draft) Act on Promotion of AI Industry and Framework for Establishing Trustworthy AI is currently awaiting the National Assembly's final vote. Once this is passed, the law could take effect within 2023 or 2024. Although the full text of the act is not yet available to the public, it is reported to comprise and incorporate seven previous sets of legislation. A fundamental tenet of this law is that anyone should be allowed to develop new AI technology without having to obtain government pre-approval. This law also identifies high-risk AI – for which there are stricter requirements that need to be met. An AI committee will also be constituted, presumably to administer and enforce provisions of the act.
- The (Draft) Royal Decree on Artificial Intelligence System Service Business in Thailand is awaiting revisions following a public consultation in October 2022. This decree adopts a risk-based approach and identifies prohibited versus high-risk AI. It imposes specified conformity assessments on high-risk AI systems; in contrast, limited-risk AI need only fulfil certain transparency requirements (which could encompass reporting to the authority). AI providers located outside of Thailand but providing services in Thailand must appoint a local representative and be registered with the Thai authority. It was clarified that the decree will not apply to AI systems under the supervision of sectoral regulators, e.g., the Bank of Thailand and the Office of the Securities and Exchange Commission, provided transparency and fairness standards are in place that are no lower than those under the decree.



Charmian Aw
Partner, Data Privacy, Cybersecurity & Digital Assets
Singapore

The AI Landscape in the UK

Geopolitics

In March 2023 the UK government published its policy paper, "A Pro-innovation approach to AI Regulation". The paper seeks to carve out a distinct path for post-Brexit UK as a global leader in AI, making the UK "the best place to research AI and to create and build innovative AI companies". While the EU seeks to implement a comprehensive AI Act, with rules and obligations calibrated according to risk levels, the UK government is seeking to benefit from its separate status by pursuing a combination of:

- Multilateral engagements with bodies such as the OECD AI Governance Working Party (AI-GO), the Council of Europe Committee on AI (CAI) and Global Standards Development Organisations.
- Bilateral AI engagement with individual nations and jurisdictions as they develop regulatory and governance approaches to AI. These bilateral engagements include the EU and its individual member states, the US, Canada, Singapore, Japan, Australia, Israel, Norway and Switzerland.

The UK government's explicit objectives include promoting interoperability and coherence between different approaches and using its "world-leading innovation provisions in free trade agreements to address the challenges innovators in AI may face and ensure that businesses are able to take advantage of the opportunities it presents".

The UK government sees agility and "light touch" regulation as the key to innovation and competitive advantage. Rather than developing comprehensive legislation and creating a single regulator, the UK's approach is to require existing regulators to adopt approaches suited to its actual use in their sectors, and to rely on existing laws where enforcement action is required. This approach cuts against global trends towards detailed, unified and economy-wide laws and regulation. It remains to be seen whether the result is to establish the UK as an attractive venue for innovation and inward-investment, or whether its patchwork of laws and sector-focused regulators, as well as its status as an outlier in global regulatory terms, are perceived as costly and difficult to navigate. It is a bold approach that will either prove the case for agility or confirm the need for simplicity and regulatory coherence.

Technology

The UK policy paper highlights the already wide and rapidly increasing range of technologies through which AI is being deployed. The pace and diversity of AI development underpins the UK government's view that it would be a mistake to define and seek to regulate AI by assigning rules or risk levels to entire sectors or technologies. Instead, the UK seeks to "regulate based on the outcomes AI is likely to generate in particular applications". To support that approach, the UK will define and identify AI by reference to two characteristics:

- **Adaptivity** – AI systems' ability to infer patterns and connections in data not easily discernible to or envisioned by humans.
- **Autonomy** – The capacity of AI systems to make decisions without express intent or ongoing human control.

UK regulators will be required to identify AI through those characteristics and to assess risk in context and by reference to use, not technology. For example, "an AI-powered chatbot used to triage customer service requests for an online clothing retailer should not be regulated in the same way as a similar application used as part of a medical diagnostic process". Having identified AI, regulators would be required to assess specific risks in terms of:

- Safety, security and robustness
- Appropriate transparency and explainability
- Fairness
- Accountability and governance
- Contestability and redress

Opportunities and Risks

The UK government has emphasised the scale of economic opportunity that comes with AI, pointing to its £3.7 billion contribution to the UK economy in 2022. However, critics including civil liberties groups and technology institutions point to the attendant risks. They include:

- The risk of bias and discrimination stemming from the large datasets used to train AI models
- The risk that AI can be used to spread and amplify disinformation and "fake news"
- The risk that generative AI and other AI applications could threaten jobs
- The risk that AI-driven surveillance, including facial recognition, biometric identification and "social scoring", could undermine privacy and civil liberties
- The risk that the complexity and opacity of AI systems could lead to decisions being made in relation to individuals or groups with no clear explanation of the decision-making process or a route to contestability or redress

The EU approach relies on legislation to implement a rules-based approach to AI governance. The UK's post-Brexit approach, specifically differentiated from the EU, is to adopt a "contextual, sector-based regulatory framework", anchored in its existing, diffuse network of regulations and laws.

In addition to concerns about the proposed "patchwork" approach to regulation, organisations such as the Ada Lovelace Institute have criticised elements of the UK's Data Protection and Digital Information Bill (Bill), currently under consideration by Parliament. In their July 2023 report "Regulating AI in the UK", Matt Davies and Michael Birtwhistle urged the UK government to rethink elements of the Bill that are "likely to undermine the safe development, deployment and use of AI". Those elements include amendments to UK GDPR Article 22, which would remove the prohibition on many types of automated decision-making, instead requiring data controllers to have safeguards in place, such as measures to enable an individual to contest the decision. The report's authors also observe that the Bill would remove the obligation to carry out a data protection impact assessment when high-risk processing is being carried out. The Bill is a "deregulatory proposal that is intended to reduce the burden on businesses of complying with data protection law". Set against that pro-innovation objective is the Bill's potential to weaken protections currently enjoyed by individuals. The report's authors conclude: "Against an already-poor landscape of redress and accountability in cases of AI harms, the Bill's changes will further erode the safeguards provided by underlying regulation."

The current UK government is unlikely to be swayed by such expression of concern. Its clearly articulated position places great emphasis on post-Brexit freedoms. The ministerial foreword to the March 2023 policy paper confidently asserts, "Having exited the European Union we are free to establish a regulatory approach that enables us to establish the UK as an AI superpower. It is an approach that will actively support innovation while addressing risks and public concerns. The UK is home to thriving start-ups, which our framework will support to scale-up and compete internationally. Our pro-innovation approach will also act as a strong incentive when it comes to AI businesses based overseas establishing a presence in the UK."

Malcolm Dowden
Co-head of Knowledge Management, Data Privacy, Cybersecurity & Digital Assets,
London

The AI Landscape in Europe

The EU has proposed its first regulatory framework for artificial intelligence (AI Regulation Proposal) as part of its digital strategy, one of the European Commission's political priorities for 2019 to 2024. This proposal is aligned with the EU's values, fundamental rights and principles, having a human-centric approach. This means that the regulation aims for AI not to be an end by itself, but to serve people and increase human wellbeing.

To achieve this, the trustworthiness of AI should be ensured throughout the EU. To do so, the EU has opted for a regulation as a legal instrument, which reduces legal fragmentation and facilitates the development of a single market while leaving some room for different levels of member state action for elements that do not undermine the objectives of the initiative.

It also goes a step further in terms of its reach, as it has an extraterritorial scope, meaning that it will apply to (1) those providers placing on the market or putting into service AI systems in the EU, irrespective of whether those providers are established; (2) those users of AI systems located within the EU; and (3) providers and users of AI systems that are located in a third country, where the output produced by the system is used in the EU.

As per its material scope, the definition of what should be considered AI under the proposal is quite broad intentionally, to ensure that the AI Regulation text remains flexible and future-proof. It also shows that the focus of this regulation is less about the underlying technology or algorithms, but more about establishing a framework for the ethical and human-centric development of AI systems in the EU. According to the proposed act, the different AI systems will be analysed and classified based on the risk they pose to users and will have obligations proportionate to the level they are in. There are four different levels of risk: (1) unacceptable risk, (2) high risk, (3) limited risk and (4) low risk.

The primary challenge for the AI Regulation Proposal is that European legislative processes are slow, but AI is evolving rapidly, so there is some concern that the regulation could be outdated by the time it comes into force (it is expected to be adopted this year and will come into force about two years after adoption, potentially in late 2025 or early 2026).

This has led the European Commission and private entities to develop voluntary frameworks such as the AI Pact, aimed for both EU and non-EU companies to commit to voluntary and early implementation of key provisions of the AI Regulation Proposal before it is implemented, or the AI Code of Conduct, again, aimed at reaching voluntary commitments aligned with the principles of the AI Regulation Proposal on Generative AI.

Further issues are present in connection with the AI Regulation Proposal, such as the fact that, in the worst-case scenario, there would be no agreement between the European institutions on the final text, or that the final text would overlap with aspects connected to AI technology covered by other regulations, for instance, on privacy, IP, free use of data or cybersecurity, resulting in duplicative or conflicting rules that would make them difficult to implement, construe or enforce.

Finally, it is evident that the use of AI generates both risks and opportunities for organisations. In our view, AI becoming mainstream highlights the need to prioritise the training of professionals, as it is essential that they understand the capabilities, limitations and risks of AI, as well as the ethical and legal aspects associated with its implementation. Furthermore, businesses will encounter the challenge of implementing robust procedures for data and AI governance that ensure compliance with upcoming laws and regulations.

Charles Helleputte
Partner, Data Privacy, Cybersecurity & Digital Assets
Brussels/Paris

The Ethical Conundrum

The potential game-changing promise of AI comes with the realisation that these systems also pose several real and important risks. What is clear is that we need to proceed cautiously to ensure that while we are capturing the advantages of AI, we are also managing the risks.

It is recognised that risks arise in areas such as the ability of AI to generate human-like content, such as deepfakes of people, and false information. This risk, as well as the risk of biases being perpetuated by AI outcomes, are factors that need to be carefully addressed. These risks, in particular, can be seen to create greater challenges because, while as a society we are becoming more sceptical of online content, AI may not be able to apply the same scepticism. Although AI output can be seen to have greater scientific rigour and an impression of objectivity, the reality can be very different.

Furthermore, as AI systems need data, and lots of it, key risks exist around data privacy and copyright and the use of outputs that use sensitive data and/or products that are the result of a person's copyright or other IP being infringed.

All these risks are important, but a different yet equally important challenge posed by AI is that as machines drive productivity, it is usually at the expense of humans who were initially carrying out those tasks. AI will likely transform sectors of the workforce and as society moves forward with embracing the benefits of AI, there is a need to ensure that the workforce is reskilled or upskilled in order for people to be able to participate in this process.

When developing an AI strategy, businesses should consider establishing an AI governance framework to guide their investment process and reduce any ethical, legal or regulatory risks. They should also incorporate data security measures, as a breach would be both reputationally and systematically detrimental and impede public trust. Finally, the strategy should establish control of the systems, clearly identifying risk frameworks, contingency plans and a point of responsibility in the event of an error. [16] We provide more guidance around this in our AI Governance Toolkit on p.36.

Australia's Artificial Intelligence Ethics Framework

In place of a direct regulatory approach, the Australian government was one of the first governments in the world to produce AI ethics principles, which were released in 2019 and align with the international standards set out by the OECD.

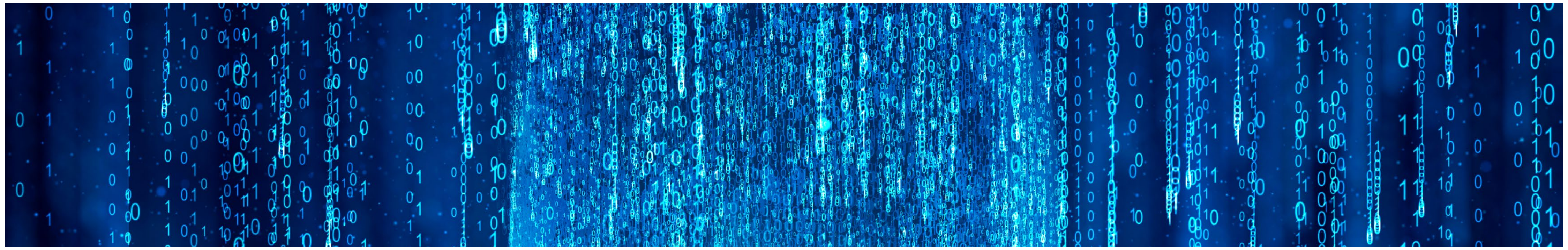
There are eight voluntary principles that the government recommends businesses comply with when developing, implementing and distributing AI products. Those principles are tied to how AI impacts the individual, society and the environment. They include that:

- They should respect human rights, autonomy and the diversity of individuals
- They should benefit individuals, society and the environment
- They should be inclusive and accessible, and they should not involve or result in unfair discrimination against individuals, communities or groups
- They should respect and uphold privacy rights and data protection, and the security of data
- They should reliably operate in accordance with their intended purpose
- There should be transparency and responsibility around disclosure so that people understand when they are interacting with, or impacted by AI, and can find out when an AI system is engaging with them
- When AI significantly impacts a person or a community group, there should be a timely process that allows people to challenge the AI outcomes
- The people responsible for the different phases of the AI system life cycle should be identifiable and accountable to the outcomes of the AI systems

In Australia, these AI Ethics Principles are currently working with a range of existing laws of general application to seek to address some of the risks of AI, including ethical risks. Whether this remains the approach or whether more specific laws are introduced is a matter that is currently under consideration.

[16] Accenture, "Artificial Intelligence".

2. AI in Practice



Legal Practice: Using Artificial Intelligence for Greater Efficiency and Innovation

The way business operations have evolved in the last 20 years has resulted in masses of electronic data and documents being generated every day.

Law firms are having to deal with ever increasing volumes of client data, which is highlighting a need for technology to assist to collate, organise and process this data so that it becomes manageable. AI is set to become essential for law firms to not only manage client data, but also to review it and apply it to the legal issues.

Many, in the legal profession in particular,[17] consider AI to be new technology and something scarcely understood. The reality is that many lawyers already use different types of AI in their practice, perhaps unknowingly. Rather, it is the generative AI they associate with the new and unfamiliar technology. There is a lot that AI already offers law firms, and looks to be capable of offering soon to reduce client costs and improve efficiency.

Where AI Is Already Being Used?	
Discovery	A common use of AI technology is in electronic discovery (e-discovery). This is a subset of machine learning AI,[18] which involves feeding data into a platform, setting rules and parameters, then processing the data and providing results that respond to those parameters. Lawyers then review the batches of documents produced by the system applying the inputted rules. Beyond this process, Technology Assisted Review (TAR) software is an AI technology that automatically reviews documents by combining predictive coding, a technology that produces a relevance score for documents using algorithms, with human expertise.[19] TAR is continually evolving to incorporate more powerful analytic software to e-discovery platforms. Some would argue that the technology removes the risk of documents being missed, which is a risk carried with manual review, but the sophistication in technology allows for links to be identified in datasets that may not have been contemplated.
Legal Research	The ability to identify precedents and authorities is key to many areas of legal practice. These areas are usually heavily reliant on global legal research platforms that provide access to comprehensive collections of legal resources and publications. The citations feature of these platforms helps users verify the validity and history of case law. These platforms are traditionally known for using natural language processing and machine algorithms to analyse legal texts, understand content and provide suggestions based on a user's queries. The legal profession is already well accustomed to electronic research tools, which are utilised to find the best authorities on legal topics in short amounts of time. The newer AI technologies emerging are combining authority grading with legal commentary processing to be able to answer legal research questions with supporting authorities. Some AI technologies in the US promote having advanced case authority analytics to an extent that they can identify patterns in case law and predict likely outcomes of cases or behaviour of judges. If accurate, this technology could be capable of delving into prospects analysis for cases, something that usually takes a lawyer years of experience to develop as a skill.
Generative Platforms	There is currently more limited use of generative AI platforms in Australia for legal work. Generative AI, the most well-known being ChatGPT, has better capabilities for formulating and generating content and correspondence such as letter or emails with a high degree of accuracy. However, as outlined here, the automated drafting of legal documents is still in its infancy.

[17] Thomson Reuters Institute, "ChatGPT and Generative AI within Law Firms", (online at 19 October 2023)

[18] Deloitte, "Artificial intelligence and machine learning in e-discovery and beyond", (online at 19 October 2023).

[19] G. Kelly and J. Bourke, Lexology, "AI in e-Discovery – Just How Smart Is It?" 24 January 2023.

Opportunities Presented by AI	
Efficiency	Arguably, where AI has been most effective to date in Australia in improving efficiency, is with e-discovery platforms. These platforms are reducing document review times and enable searches to be run that would not ordinarily be possible through manual review. Additionally, the technology is argued to reduce the risk of documents being missed through human error, although there is little doubt that risk still exists, as ultimately humans are still reviewing the batches of documents produced using these programmes. The result is that lawyers can cut through much more data than would otherwise be possible using these programs.
Costs Saving	Costs saving remains the biggest potential advantage being promoted as flowing from AI programmes. If software providers were to deliver on their promises, once trained, the software could provide potentially significant reductions in the time required to process data and produce a result. In its most basic form, if a firm is charging by the hour, saving time will result in a cost saving for the client. Another category of cost savings might be where these platforms offer multiple capabilities in addition to their base functions, for instance, the ability to run personal property securities register searches or company searches while building contracts. Law firms will no longer need third-party providers for these services. While this may sound appealing for bigger firms, with deeper pockets, that are able to front the initial costs of implementing the technology, this may not be viable for smaller firms with smaller clients, unwilling to fit the bills. There is little published information available yet on the true costs of utilising AI. Finally, if AI technology replaces those tasks traditionally carried out by numerous paralegals and junior lawyers, the role for these employees will change. It will see law firms needing more technology support staff, rather than junior lawyer staff, to oversee the AI technology.

How Is This Evolving and What Opportunities Are Emerging?

There is a substantial volume of online marketing material pitching AI software with capabilities specifically tailored to law firm needs. Providers are claiming to have advanced the technology beyond the existing AI uses described here, to be capable of undertaking more substantive legal analysis and producing legal documents. While the extent to which these are currently available in Australia or suitable to practice in Australia is unclear, the capabilities claimed by these platforms present a multitude of potential opportunities to the Australian legal sector, some of which are examined below.

Contract AI Software

Contract analysing AI software is an existing category of technology that originated as a basic catalogue-based system (containing a repository of ready-drafted clauses). New technology is now being advertised as having the ability to draft and produce tailored contracts from a repository of clauses and has analytic capabilities that enable it to process clause wording to identify key contract terms and inconsistencies. It is also said to have corrective capabilities where it can classify undefined terms, inconsistent terminology and identify any missing conditions or clauses. These platforms are also said to be capable of automating the application of amendments and automatically diarising key contractual dates. This, in turn, acts as a valuable tool in providing consistency and minimising legal risks for law firms and their clients.

How effective this software is needs to be further investigated. However, if such software was effective, there would seem to be significant opportunities in practices traditionally dealing with high volumes of standard form contracts in the real estate sector, such as dealing with leases, deeds, mortgages and purchase agreements. Other practice areas, such as corporate M&A, dealing with large streams of due diligence could benefit from technologies that can automate parts of the due diligence process for lawyers.

There is limited information on the ability of such software to draft court documents, such as affidavits and simple witness statements. If online information is to be believed, it appears that the technology is being used in the US for court document drafting. However, it is unknown the extent to which this is currently being used in Australia.

Capitalising on AI

AI presents a multitude of opportunities for legal firms and legal practice, including potential improved client satisfaction by increasing practice efficiency, reducing billables for labour intensive tasks and efficiently identifying issues and risks in legal matters. Law firms embracing AI technology early may have the opportunity to take on bigger client files and build breadth and depth of expertise in this area. AI seems to present an opportunity to elevate client services and stay ahead in an increasingly competitive market, but the reality of that is arguably yet to be embraced.

What Opportunities Are There for Law Firms?

While fundamentally the attraction of utilising technology in legal practice begins with saving time and increasing accuracy, there are several other potential benefits to law firms utilising AI for their practice. If AI technologies (in particular generative AI) take hold, they have the potential to reshape the traditional law firm and provide better services to clients.

Case Study

Can Artificial Intelligence Be an "Inventor"?

The Thaler cases appear to be the first Australian cases that have directly grappled with issues arising out of the use of AI and, specifically, their intersection with IP rights.

Dr. Stephen Thaler (Thaler) brought an action in the Federal Court in 2021,[20] seeking judicial review of a decision of the Deputy Commissioner of Patents (Commissioner) to deny his patent application.[21] The application was denied because the Commissioner determined that an AI system named DABUS (an acronym for device for the autonomous boot-strapping of unified sentience) could not be considered an "inventor" under the Patents Act 1990 (Cth) (Act).

Beach J set aside the Commissioner's decision.[22] In construing the term "inventor", His Honour took a progressive approach, criticising the "mere resort to old millennium usages of that word".[23] Further, if a human inventor is required by the Act, then in circumstances where an AI system created the invention, it could not be patented and, therefore, may not be disclosed to the public.[24] This, in Beach J's opinion, would be antithetical to the objective of the Act, being the promotion of innovation.[25] On the other hand, allowing computer inventorship would incentivise the development of creative machines by scientists, the use of output of such machines and the discovery of new scientific advantages.[26]

However, Beach J's decision was overturned on appeal to the Full Federal Court.[27] The Full Court found that His Honour's consideration was clouded by the broader question of the role AI should have within the Act.[28] It said that question did not bear on the proper construction of section 15(1) of the Act.[29] In relation to the meaning of "inventor", the Full Court said that references to a "person" in the Act were not necessarily references to a human person.[30] However, a person's entitlement to a patent is premised on an invention that has arisen out of the mind of a natural person or persons.[31] An "inventor" must, therefore, be a natural person.[32] The Full Court also rejected the notion that if DABUS is not accepted as the inventor, no invention devised by an AI system can be granted a patent. It said that the characterisation of a person as an inventor is a question of law, and that whether the invention has a human inventor (i.e. Thaler) has not been explored in the litigation and remains undecided.[33] The Full Court also observed that there are many propositions that arise for consideration in the context of AI and inventions, but appeared to indicate these are policy questions to be decided by parliament.[34]

Thaler applied for special leave to appeal to the High Court. The court refused the application on the basis that the matter was not the appropriate vehicle for considering the issues of principle sought to be agitated by Thaler.[35]

This spells the end of Thaler's case in Australia, which is in line with the outcomes of proceedings that Thaler brought in other common law jurisdictions such as New Zealand,[36] the US,[37] and the UK[38] (although those decisions were based on the particular statutory words used in those jurisdictions). In contrast, Thaler's application for a patent was successful in South Africa.[39] However, there appear to be differing views as to whether this was a mere oversight by the patent office, or a deliberate decision made to reflect South Africa's push to increase innovation.[40]

Interestingly, in June 2022 and following the UK Court of Appeal's judgment[41] in Thaler's case,[42] the UK government concluded its consultation on AI and IP, deciding that for "AI-devised inventions, we plan no change to UK patent law".[43] Most respondents viewed AI as a tool that is incapable of inventing without significant human intervention.[44] This meant most viewed the UK's current patent laws as being adequate to protect inventions created with the assistance of AI.[45] However, the UK government acknowledged that it would be best to move forward with the intention of harmonising any change in its rules at an international level to support its economic interests and competitive edge.[46]

This and the Full Court's judgment suggest that in future cases dealing with AI, common law courts (such as those in Australia) are likely to leave any advances in the law with regard to the recognition of AI in the hands of the legislature. However, in the absence of legislative developments, there remains a potential for the High Court to consider the issues raised by Thaler, should there be an appropriate vehicle in which to do so.

[20] *Thaler v. Commissioner of Patents* [2021] FCA 879.

[21] *Stephen L. Thaler* [2021] APO 5 (9 February 2021).

[22] *Thaler v. Commissioner of Patents* [2021] FCA 879.

[23] Ibid [15].

[24] Ibid [130], [132].

[25] Ibid [124].

[26] Ibid [13], [124]-[125]. As stated in s 2A of the Act, the object of the Act is to "provide a patent system in Australia that promotes economic wellbeing through technological innovation and the transfer and dissemination of technology" which "balances over time the interests of producers, owners and users of technology and the public".

[27] Commissioner of Patents v. Thaler [2022] FCAFC 62.

[28] Ibid [119].

[29] Ibid.

[30] Ibid [105].

[31] Ibid. See also at [116].

[32] Ibid [106], [108], [113].

[33] Ibid [121].

[34] Ibid [119]-[120].

[35] *Thaler v. Commissioner of Patents* [2022] HCATrans 199 (11 November 2022), page 15.

[36] See *Thaler v. Commissioner of Patents* [2023] NZHC 554 at [29]-[33], where the NZ High Court found that AI cannot be considered an "inventor" for the purposes of the Patents Act 2013 (NZ) because it is not a person. While the Patents Act had been passed when AI was known, the court found that there was nothing in the legislative history to indicate that parliament intended to open up the possibility of AI being an inventor (see at [2]).

[37] Earlier this year, the US Supreme Court declined to hear Thaler's appeal of the US Court of Appeals' decision in *Thaler v. Vidal*, 43 F.4th 1207 (Fed. Cir. 2022). Both the appeal decision and the first instance decision in Virginia (*Thaler v. Hirshfeld*, No. 1:20-cv-903, 2021 WL 3934803, at *2 (E.D. Va. Sept. 2, 2021)) upheld the decision of the US Patent and Trademark Office to reject Thaler's patent application because US patent law requires "inventors" to be human beings.

[38] Thaler's case was most recently heard by the UK Supreme Court, with the decision pending. It is an appeal of the UK Court of Appeal's judgment in *Thaler v. Comptroller-General of Patents, Trade Marks and Designs* [2021] EWCA Civ 1374, which found that DABUS could not be considered an "inventor" for the purposes of the Patents Act 1977 (UK) because it is not a person.

[39] Naidoo, Meshandren, "In a world first, South Africa grants patent to an artificial intelligence system", 5 August 2021, the Conversation <https://theconversation.com/in-a-world-first-south-africa-grants-patent-to-an-artificial-intelligence-system-165623>.

[40] Ibid.

[41] *Thaler v. Comptroller-General of Patents, Trade Marks and Designs* [2021] EWCA Civ 1374.

[42] But before a scheduled hearing of an appeal to the UK Supreme Court in March 2023.

[43] UK Intellectual Property Office, "Artificial Intelligence and Intellectual Property: copyright and patents: Government response to consultation" (28 June 2022) at [87] (https://www.gov.uk/government/consultations/artificial-intelligence-and-ip-copyright-and-patents/outcome/artificial-intelligence-and-intellectual-property-copyright-and-patents-government-response-to-consultation).

[44] Ibid [69].

[45] Ibid [79].

[46] Ibid.

3. Embracing AI

Recognising and Mitigating AI Legal Risks

There are a number of significant legal risks for businesses to consider when adopting and using AI tools and systems (particularly generative text). Here we touch on how to control and mitigate risks to avoid compliance breaches and complex legal issues.

Key legal risks discussed include:

- Misinformation
- Bias and unlawful discrimination
- IP infringement
- Data privacy breaches
- Cybersecurity and other illegal activity

Misinformation

AI systems, such as generative text tools, can generate or propagate false information, which can have consequences for businesses that permit staff to use these tools.

Take, for example, the New York-based lawyer who relied on ChatGPT for legal research in a personal injury case, and failed to appreciate the extent to which ChatGPT could fabricate information and submitted fake case citations that had been generated by AI in a brief to the Federal District Court. The judge found the lawyer made false and misleading statements to the court, and he was fined US$5,000 and was required to notify each real judge who was falsely identified as the author of the fake cases.

Businesses in the publishing sector will be alert to misinformation risks, including defamation risks associated with generative text AI tools. In Australia, there was an instance where ChatGPT falsely stated that a Victorian mayor was convicted of foreign bribery offences, when, in fact, he had been the whistleblower.

Generative text AI tools are not connected to the internet and are not search engines, although the two types of technologies are becoming more integrated.[47] Generative text tools have limited knowledge of world events, and only contain information up to a certain date by which they were trained. They are probabilistic models and, therefore, sometimes produce incorrect information or fabricated content.

On its website, OpenAI warns in relation to ChatGPT that "outputs may be inaccurate, untruthful, and otherwise misleading at times."[48] It further states: "We'd recommend checking whether responses from the model are accurate or not."[49]

Under ChatGPT's terms (comprising service terms,[50] terms of use,[51] a sharing and publication policy[52] and usage policies[53]), the user owns all content input and ChatGPT assigns to the user all rights, title and interest in and to the content output. Further, the user is contractually responsible for ensuring that the content does not violate any applicable law or the terms.

However, attempts to shift liability to the user are unlikely to be an effective legal defence for companies that own or operate AI technology in instances where there is a breach of a statutory duty or obligation that cannot be contracted out of, including, for example, defamation law in Australia.

It is important for businesses to carefully consider whether they permit the use of generative text tools for work purposes, and if they do, for people to be cautious and critical when using or publishing AI-generated content and to verify information independently, especially in situations where accuracy is crucial.

[47] For example, in February 2023, Microsoft unveiled a new version of its search engine, Bing, which is powered by an upgraded version of the same AI technology that underpins ChatGPT: https://www.theverge.com/2023/2/7/23587454/microsoft-bing-edge-chatgpt-ai.

[48] https://help.openai.com/en/articles/6783457-what-is-chatgpt.

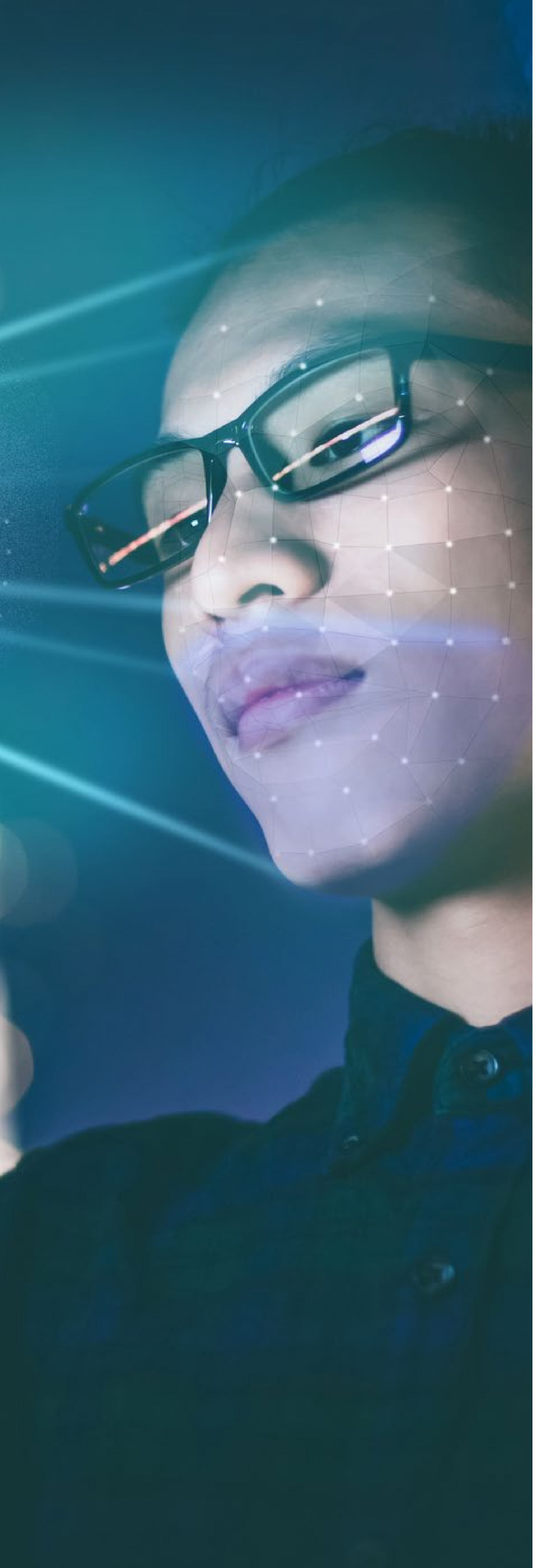
[49] Ibid.

[50] https://openai.com/policies/service-terms.

[51] https://openai.com/policies/terms-of-use.

[52] https://openai.com/policies/sharing-publication-policy.

[53] https://openai.com/policies/usage-policies.



Bias and Unlawful Discrimination

Even though AI systems are generally intended to remove the subjective interpretation of data, in some instances generative text tools and AI algorithms[54] can potentially perpetuate biased information, which can have negative consequences for businesses, including creating unlawful discrimination risks.

Experts suggest that there is no such thing as neutral data. AI algorithms and generative text tools can produce biased information due to algorithmic design or if the data they are trained on was biased in the first place. This could lead to instances of biased hiring or lending practices, for example, which could contravene antidiscrimination laws and attract legal penalties. It is conceivable that a hiring algorithm, based on analysing previous decisions, could potentially discriminate against female candidates for CEO roles, for example.[55]

There are also some concerns about the extent to which minority groups might be disadvantaged when AI is used in healthcare settings if datasets are based on data predominantly from white people. The Imperial College of London has been researching this issue and has released a report.[56]

To minimise discrimination and ensure fairness, it is important for businesses, including those that create AI, to invest in the development of diverse training datasets and unbiased algorithms. Businesses should be attuned to the risk of potential bias and test and monitor their AI systems.

[54] AI algorithm is set of instructions or rules used to solve a specific problem or perform a particular task.

[55] https://www.washington.edu/news/2015/04/09/whos-a-ceo-google-image-results-can-shift-gender-biases/.

[56] O'Brien, N, Van Dael, J, Clarke, J, Gardner, C, O'Shaughnessy, J, Darzi, A, Ghafur, S., "Addressing racial and ethnic inequities in data-driven health technologies", report dated 24 Feb 2022

IP Infringement

The use of generative AI is rapidly changing the way content is created. A key issue for businesses that use generative text, or that create word marks or design marks using AI, is whether the use and collection of data in generative AI could potentially infringe copyright or trademarks, in which case businesses may one day face legal challenges from IP owners.

The precise scope and nature of the risks of infringement within generative AI are still being learned. However, according to the Australian Publisher's Association, it is undisputed that some of the most significant AI tools to date, including ChatGPT, have been trained on content without acknowledgement or permission from the original creators. For instance, a number of Australian authors were upset to discover in September 2023 that their works had been potentially pirated by the US-based "Books3" dataset and used to train generative AI for corporations such as Meta and Bloomberg.[57]

Several IP proceedings, including class actions, have commenced in the US by copyright owners against owners of generative AI for alleged copyright infringement. The results of cases are yet to be seen. It will be interesting to see whether copyright-owner plaintiffs will be able to overcome significant evidentiary hurdles to prove that a particular work in which they hold copyright was used to train an AI system. It may be that the law will need to be changed in due course to make it easier for plaintiffs to make out their cases. As noted by the Australian Publisher's Association, copyright infringement "is a massive legal and ethical challenge for the publishing industry and for authors globally".[58]

Businesses will note that from ChatGPT's perspective, pursuant to its Sharing and Publication Policy, a user is permitted to publish the content generated by ChatGPT, so long as:

- The publication is attributed to the user's name or company
- The role of AI in formulating the content is clearly disclosed and easy to understand
- Topics of content do not violate the content policy or terms of use[59]

Accordingly, ChatGPT seeks to avoid liability for potential IP infringement when a user publishes generative text.

ChatGPT further argues that fair use doctrines permit the training of AI based on original works. It appears that ChatGPT's position (as reportedly argued in a US IP-related legal proceeding) is that authors may "misconceive the scope of copyright, failing to take into account the limitations and exceptions (including fair use) that properly leave room for innovations like the large language models now at the forefront of artificial intelligence."[60]

Businesses and people around the globe who publish generative text or marks will want to keep an eye on international IP case law developments and legislative changes to see how cases pan out.

[57] As reported by *The Guardian* on 29 September 2023: https://www.theguardian.com/australia-news/2023/sep/28/australian-books-training-ai-books3-stolen-pirated?CMP=oth_b-aplnews_d-3.

[58] A quote by Stuart Glover, spokesperson of the Australian Publisher's Association: https://www.theguardian.com/australia-news/2023/sep/28/australian-books-training-ai-books3-stolen-pirated?CMP=oth_b-aplnews_d-3.

[59] https://openai.com/policies/sharing-publication-policy.

[60] https://www.theguardian.com/australia-news/2023/sep/28/australian-books-training-ai-books3-stolen-pirated?CMP=oth_b-aplnews_d-3

Data Privacy Breaches

AI systems typically hold vast amounts of complex data, raising concerns about the collection, storage and use of personal information. A data breach, occurs when personal information that an entity holds is subject to unauthorised access or disclosure or is lost.

AI systems that collect, store and use personal information, for example, must be carefully designed to protect data privacy. Specific risks include that AI systems, through advanced analytics, might infer sensitive details about individuals or might fail to anonymise personal data. Businesses that use AI systems ought to consider the increased risks of non-compliance with privacy and data protection regulation in their relevant jurisdictions and implement additional controls to ensure the robustness of AI systems. Encryption and access controls, for example, can be used to safeguard private data in AI systems.

In the event of a breach, businesses that are covered by the Privacy Act 1988 (Cth) in Australia[61] will be aware that they must report an eligible data breach[62] to the Office of the Australian Information Commissioner (OAIC) under the Notifiable Data Breaches scheme, and notify the individuals concerned. Notifications must include a description of the data breach, the kinds of information involved and recommendations about the steps individuals should take in response to the data breach.[63] If businesses experience a data privacy breach, they will need to demonstrate to regulators (and in any civil actions brought against them) that they took reasonable measures to protect the personal information they held from misuse, interference, loss, unauthorised access, modification or disclosure.

Cybersecurity Breaches and Other Illegal Activity

AI tools may be susceptible to manipulation by cybercriminals, leading to threats that can disrupt business systems and potentially create serious damage. There have been several significant cybersecurity breaches in Australian organisations where cybercriminals have infiltrated systems (Optus, Medibank, Latitude, ANU, etc.). It is not known if the cause of the breach was use of AI.

Businesses and individuals should be aware that it is possible for cybercriminals to utilise AI such as generative text tools to draft highly personalised spear-phishing messages that appear real. Staff need to be proactively educated and trained about such risks. In the ANU case, cybercriminals utilised spear-phishing campaigns to procure network access credentials from staff. A single staff member opened an infected email, which granted the cybercriminals deep levels of access and breached the university's enterprise systems domain so that people's personal information became accessible.

Generative text tools could also be used to generate code or content that contains malware or exploits vulnerabilities in software or systems. They could also be used to generate scam offers, fraudulent schemes or deceptive advertisements designed to exploit victims.[64]

Businesses ought to conduct risk analyses and audits, invest in strengthening their cybersecurity infrastructure and educate their staff on how to deal with cyberthreats.

Businesses can also investigate the ways in which AI can be used proactively as a tool to combat cyberthreats, including identifying threats in the first instance and improving response times.

[61] Relevantly including organisations with an annual turnover more than $3 million.

[62] An eligible data breach occurs when the following criteria are met: (1) there is unauthorised access to or disclosure of personal information held by an organisation or agency (or information is lost in circumstances where unauthorised access or disclosure is likely to occur); (2) this is likely to result in serious harm to any of the individuals to whom the information relates; and (3) the organisation or agency has been unable to prevent the likely risk of serious harm with remedial action: https://www.oaic.gov.au/privacy/notifiable-data-breaches/report-a-data-breach.

[63] https://www.oaic.gov.au/privacy/notifiable-data-breaches/report-a-data-breach.

[64] These examples are sourced from ChatGPT itself.

Mitigation and Control of Risks

As outlined above, there are many risks to consider when managing the use of AI, including the risks of misinformation, bias, unlawful discrimination, IP infringement, data privacy breaches and cybersecurity-related risks.

Businesses should weigh up the risks and opportunities of using AI and decide the extent to which AI will be permitted and implemented in their organisations. To align with best practice and legal compliance, businesses should ensure mitigating processes are put in place as soon as AI systems are implemented and many businesses will require an AI governance policy and framework.

Importantly, AI policies should reflect that there is a need for human oversight of AI, and that humans should bear ultimate responsibility for the use of AI-generated content.

Businesses should also consider how existing laws and regulation apply to their AI usage, including privacy law, cybersecurity and data protection law, copyright law, consumer protection, defamation law, antidiscrimination law and tort law, among other laws.

International businesses also need to consider their international obligations, including under any relevant AI regulations. The regulatory landscape is evolving quickly and many jurisdictions (i.e. in Europe, the US and China) make AI governance systems obligatory.

It is important for businesses to understand the legal risks that can arise in the everyday use of AI, and to seek to have systems and processes that address and mitigate risks to ensure that AI is used ethically and responsibly and does not become a source of liability.

Case Study

Generative Artificial Intelligence: Creating New Text, Images and Disputes

The increasingly widespread use of ChatGPT (from OpenAI) has re-imagined the role of AI in our daily lives. There has been much discussion of the ways in which AI can be deployed. But as new questions around the legality of these systems are raised, it has become apparent that their very development and use of these systems may also be the subject of litigation. This can be seen in the recent emergence of litigation in the US, where generative AI companies, such as OpenAI, have found themselves in the firing line.

Generative AI is a type of AI that can create new and realistic content from "training data", an extensive body of information that their underlying models learn from.[65] What is remarkable about this type of AI is that the output, whether images, text or other forms of content, is coherent and often human-like. However, it is the way in which information is sourced on a vast scale, by "scraping" the internet, that has proven contentious and gives rise to the concerns some have. Key areas of law that have been considered include data protection and privacy, as well as IP. Snapshots of some of the cases presently underway are given below.

1. Copyright Infringement

- Several lawsuits have been brought against generative AI companies for copying or using data to train their AI systems, without proper attribution, consent or payment to the rightsholders.
- **Copilot lawsuit (*Doe v. GitHub, Inc.*)** – On 3 November 2022, a class action was filed by several software developers against GitHub, its parent company Microsoft and its partner OpenAI in relation to GitHub's Copilot tool, which predictively generates further code based on a programmer's existing code.[66] Copilot was trained on billions of lines of open-source licenced code that was published on GitHub's website.[67] The plaintiffs claimed that Copilot was creating from code they had written, sometimes even reproducing it, without proper attribution, thereby infringing copyright laws (among numerous other legal claims).[68] On 11 May 2023, the US District Court in California partly granted a motion to dismiss the plaintiffs' claim, dismissing numerous claims based on breach of copyright law, consumer privacy violation, tortious interference in a contractual relationship, false designation of origin, fraud, unfair competition and more (with leave to amend).[69] However, the court allowed the claim to proceed based on future harm for which injunctive relief was sought.[70] This included based on the alleged violation of the open-source licences under which plaintiffs published their code.[71]
- **Stability AI lawsuit (*Andersen v. Stability AI Ltd.*)** – On 13 January 2023, artists Sarah Andersen, Kelly McKernan and Karla Ortiz filed a class action in the US District Court in California against Stability AI, Midjourney and DeviantArt for their use of copyrighted images in training their AI image generation products without obtaining consent from those who held rights to the underlying images.[72] Further, they allege that the use of their works in training the models results in a continual production of derivative works in violation of their copyrights (with AI expressed as "a 21st-century collage tool").[73] However, the judge hearing the case recently indicated that he was inclined to dismiss most of the applicants' complaint.[74] One hurdle faced by the applicants is that the resultant images produced by Stable Diffusion do not closely resemble any given image in the training data.[75]

[65] "Generative AI", Boston Consulting Group (Web Page); Shemir Javaid, "Generative AI Data in 2023: Importance & 7 Methods", AIMultiple (Web Page).

[66] US District Court, Northern District of California, "Order Granting in Part and Denying in Part Motions to Dismiss", Doe 1 v. GitHub Inc (Case No 22-cv-06823-JST, 11 May 2023) 3.

[67] Ibid.

[68] Ibid, 3, 8.

[69] Ibid 25.

[70] bid 9-10.

[71] Ibid 10.

[72] "Complaint Class Action", Originating Process in Anderson v. Stability AI (Case No 23-cv-00201, 13 January 2023).

[73] Ibid 1 [4], 20 [90], 22 [95], 31 [160].

[74] Blake Brittain, "US judge finds flaws in artists' lawsuit against AI companies", Reuters (online, 20 July 2023)

[75] Ibid.

These issues are finding their way onto Australian shores too. It was recently reported[76] that Australian books have featured extensively in a dataset of allegedly pirated e-books known as the "Books3" corpus, which is used to train AI. This dataset was developed by independent AI researcher Shawn Presser and is alleged to include 183,000 books.[77] This dataset then became a popular dataset used to train Meta's LLaMA, Bloomberg's BloombergGPT and EleutherAI's GPT-J.[78]

In its defence, commentators, including OpenAI, have argued that training AI in this manner constitutes "fair use", as those tools do not replicate the works but produce new works, nor do they affect the market for the underlying works.[79] This is yet to be tested in court.

2. Privacy Violations

In addition to copyright infringement cases, there have been increasing concerns over the use of personal data in developing AI.

- **OpenAI lawsuit (*P.M. v. OpenAI LP*)** – On 28 June 2023, a class action was filed in the US District Court in California by anonymous consumers against OpenAI and its investor Microsoft in relation to their generative AI tools: ChatGPT, Dall-E and Vall-E.[80] Among other things, the applicants allege that OpenAI's use of personal data gathered from the internet in training its AI amounted to violations of their privacy rights.[81] OpenAI is accused of a secret large-scale web-scraping operation by gathering private information of individuals through their interactions with its products such as ChatGPT, Spotify and Microsoft Teams, without their consent. This information is alleged to include the user's photographs, locations, music tastes, financial history and others.[82]

AI algorithms draw on large volumes of data, and in doing so, pose novel legal questions. At its core, judges and policymakers must manage the tension between facilitating innovation in the technological age, and the protection of individual rights, whether IP, privacy or otherwise.

While we are in the early stages of AI litigation, it is important to remain vigilant and monitor the cases on foot, as they may shape future litigation in the US and beyond.

[76] Kelly Burke, "'Biggest act of copyright theft in history': thousands of Australian books allegedly used to train AI model",The Guardian (online, 29 September 2023); Nicola Heath, "Australian authors' works feature in Books3 dataset of pirated ebooks used to train generative AI", ABC Arts (online, 29 September 2023).

[77] Alex Reisner, "These 183,000 Books are Fueling the Biggest Fight in Publishing and Tech",The Atlantic (online, 25 September 2023).

[78] Heath, "Australian authors' works feature in Books3 dataset of pirated ebooks used to train generative AI" (n 98).

[79] OpenAI, "Comment Regarding Request for Comments on Intellectual Property Protection for Artificial Intelligence Innovation", Submission in response to US Patent and Trademark Office, Department of Commerce "Request for Comments on Intellectual Property Protection for Artificial Intelligence Innovation".

[80] PM, "Class Action Complaint", Originating Process in PM v. OpenAI LP, (ND Cal, No 23-cv-03199, 28 June 2023).

[81] Ibid 66-8.

[82] Ibid 6-7.

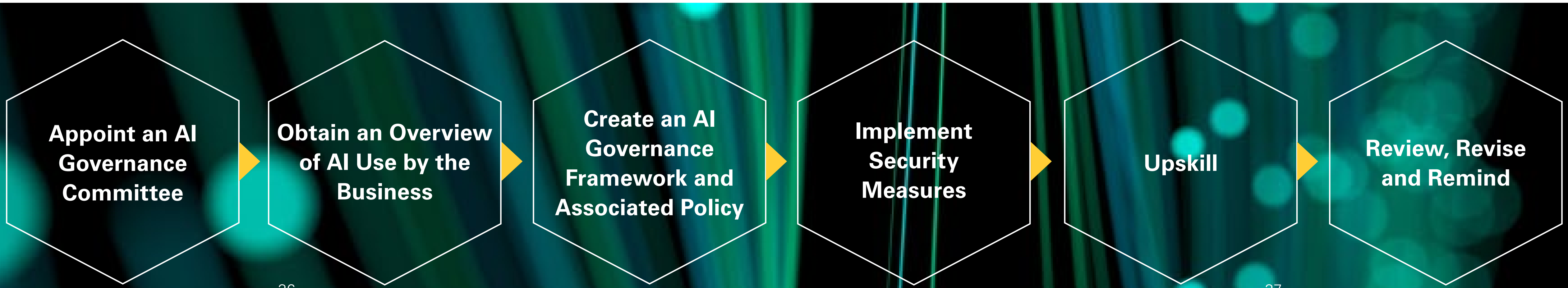
AI Governance Toolkit

Commentators consider that the AI generation could have a have a seismic impact similar to the industrial revolution.

Many business leaders find themselves in a position where they now recognise the necessity of incorporating AI into their business models, but conversations are still focused on questions around what happens next and where to start.

In order to assist businesses in managing the adoption of AI into their business operations, we detail the key considerations for business leaders.

Build AI Into Your Core Business Strategy	Business leaders need a clear and comprehensive understanding of the purpose of AI in their organisation to effectively adopt, scale and govern its use. A comprehensive understanding of the purpose of AI, and the benefits that it brings to the business, will also enable business leaders to communicate effectively with both internal and external stakeholders to foster their support and bring them along on their AI journey.
Upskill	The adoption of AI is anticipated to change the workplace as we know it, typically impacting the more administrative roles. Where possible, the workforce should be educated and upskilled in how to work with new technologies. Training is essential to ensure that any employees engaging with AI are aware of risks such as bias, false information, IP infringement, data privacy, etc.; can monitor their use of AI accordingly; and, in turn, report concerns, where necessary. This is especially important for in-house legal and compliance teams who are responsible for managing these risks. The increase in use and application of AI has resulted in a lot of new jargon floating around. Understanding the key terms and making sure that the relevant employees have a common understanding of these terms is important in understanding and assessing AI risks and developing policies. AI regulation is evolving rapidly around the world, and in the coming years we expect to see a variety of regulatory frameworks that will create a challenging landscape for businesses that act globally. In-house counsel needs to understand how regulation is evolving around the world, study AI cases in court and monitor advancements in legislation in the jurisdictions where their business operates. This not only applies to AI-specific regulation, but also the existing legislation that currently governs AI use (e.g. the Privacy Act 1998, consumer law, administrative law, IP law, the Online Safety Act 2021 and discrimination law).
Implement a Governance Policy and Framework	A policy on AI development and use, as well as a framework for applying the policy, is crucial to ensuring legal compliance, ethical processing and risk minimisation. Things to consider when developing a policy framework include the following: • Define what AI means in your organisation. Without a clear and common definition and an understanding of how your company is using AI, it will be difficult to build an AI framework. • Use existing processes and procedures to address AI risks and impact (privacy and data governance, third-party risk/vendor assessments, etc.). • Identify and involve the necessary stakeholders (IT, security, legal, HR, marketing, etc.) in the process of developing the company's policy and framework for implementation and operation. • Do not reinvent the wheel but rather review and, where appropriate, incorporate responsible AI principles from existing frameworks, such as Australia's AI Ethics Framework. • There should be transparency and responsibility around disclosure so that people understand when they are interacting with, or impacted by, AI and can find out when an AI system is engaging with them. The governance policy should establish mechanisms for effective risk assessments and management, reporting processes, and a point of responsibility for managing or resolving said risks and errors that might occur, or if AI goes wrong. These mechanisms should coincide with a documented AI response plan, which all relevant stakeholders should familiarise themselves with to respond efficiently. • Update any existing technology usage policies to incorporate AI.
Conduct Regular Risk Assessments	As discussed throughout this report, the adoption of AI comes with several potential risks. Businesses will need to review their existing risk management systems and update these frameworks to incorporate AI governance. In doing so, businesses need to set their risk tolerance in relation to AI and consider creating a risk scale to classify different types of AI usage. It is recommended that in doing so, businesses refer to risk classification systems used by regulatory frameworks such as the EU AI Act, which is considered one of the most advanced and comprehensive frameworks in existence at the time of writing. The risk management system should detail a regular timetable for risk and performance assessments, which should be more frequent during the initial introduction of AI to the business.
Data Governance	Consider how your AI governance framework will interact with your data governance framework and make any necessary updates. High-quality data is critical for AI use, so businesses need to seek to ensure that datasets are relevant to the purpose of AI, do not contain errors and are representative to avoid bias, and that, where necessary, the business has informed content to use the data. Data privacy and cybersecurity poses significant risk in relation to AI usage and at a time when the public are highly sensitive to data privacy, businesses need to be transparent about their management and use of this data. In addition, data teams need to prepare and familiarise themselves with a data breach response strategy so that they are able to act quickly if this should occur.



Appoint an AI Governance Committee

Obtain an Overview of AI Use by the Business

Create an AI Governance Framework and Associated Policy

Implement Security Measures

Upskill

Review, Revise and Remind

The Top Five Considerations for In-house Counsel Globally

Asia Pacific

1. **Data governance and mapping are key** – The risks of running afoul of data laws are heightened now that mega jurisdictions such as China and India have passed their own comprehensive privacy legislation. Even older laws are being amended to address technological advancements and evolving legal risks.
2. **Watch out for nuances in local law requirements** – While keeping closely aligned to a global baseline.
3. **Keep up to date with legislative developments and updates in Asia** – Things in this region are not only dispersed, but also constantly evolving, and it is easy to lose track. Tap into external counsel resources wherever available or possible.
4. **Prepare "heatmaps" across all relevant markets in Asia Pacific, of pertinent areas of law or issues** – This should entail not only assessing how prescriptive legal/regulatory requirements are, but also the likelihood and impact of enforcement actions or other repercussions for any non-compliance to the rules.
5. **AI governance outside of standalone legislation is vital in ringfencing risks** – Governance should be a bespoke process involving multiple stakeholders and components, including third-party contracts, internal protocols, external procedures and trainings.

Europe

1. **AI contributes to foster a digital mindset** – This will help organisations to foresee new possibilities using data, technology, algorithms and AI – make sure your organisation is prepared for continuous adaptation and change.
2. **Set a vision for using AI to further the company's business strategy** – Define and approve AI use cases and encourage employees to evaluate whether AI's strengths match up to the organisation's vision and values.
3. **Develop AI governance policies and frameworks** – This is crucial to ensuring legal compliance, adherence to ethical principles and risk minimisation.
4. **Build strong contractual coverage against liabilities when building or hiring AI solutions** – Economic and reputational risks are at stake.
5. **Stay ahead of regulatory developments** – Watch where regulation is headed and anticipate compliance actions.

US

1. **Understand the key terms** – The increase in use and application of AI has resulted in a lot of jargon floating around. Understanding the key terms and making sure that in-house teams have a common understanding of these terms is important to understand and assess AI risks and policy.
2. **Educate stakeholders on AI risks and regulation** – Although a mandatory federal AI-specific regulatory framework does not yet exist in the US, the use of AI is governed by various existing laws. In-house teams need a comprehensive understanding of how existing laws and voluntary frameworks relate to AI use in order to ensure that the business is compliant not only at the national level, but also across individual states where the business may operate. Simultaneously, where a business operates internationally, in-house teams need to monitor evolving regulatory requirements in external jurisdictions.
3. **Develop an AI governance policy and framework** – An AI policy on AI development and use, as well as a framework for applying the policy, is crucial to ensuring legal compliance, ethical processing and risk minimisation. This task is not as onerous as it seems – having assessed how your business will utilise AI, you can borrow and incorporate responsible AI principles from existing frameworks such as the NIST AI Risk Management Framework.
4. **Develop an AI governance policy and framework** – An AI policy on AI development and use, as well as a framework for applying the policy, is crucial to ensuring legal compliance, ethical processing and risk minimisation. This task is not as onerous as it seems – having assessed how your business will utilise AI, you can borrow and incorporate responsible AI principles from existing frameworks such as the NIST AI Risk Management Framework.
5. **Treat AI governance as a business and compliance imperative** – AI governance will help to avoid "legal as a roadblock" mentality and will assist your organisation in complying with existing laws and preparing for forthcoming AI-specific regulation. If your business is an AI user, legal limitations, obligations and risks, as well as reputational risks, are likely if prudent decisions are not made to ensure that the benefits outweigh the risk of harms.

UK

1. **Why is AI being deployed by your business?** Has the purpose and specific business need been identified and clearly articulated?
2. **Can your business meet the requirement of transparency and "explainability"?** In particular, is your business able to explain the system's decision-making process in an appropriate level of detail that matches the risks posed by the use of AI?
3. **Do you understand how, and from where, data used to train AI models has been acquired?** Is there a risk that the data acquisition process (e.g. through web-scraping) might have infringed IP rights? If so, do you have appropriate indemnity measures in place in case of third-party action?
4. **Does your business have accountability and governance measures in place** to ensure there is appropriate oversight of the way AI is being used and clear accountability for the outcomes?
5. **Does your business provide clear routes to dispute harmful outcomes or decisions generated by AI** to meet the UK government's requirement for contestability and redress?

The AI Era Is Upon Us

Not only does AI already feature in many people's everyday lives, but also more recently we have seen rapid advances in the capabilities of AI technologies.

Globally, governments are considering how to both regulate AI and create opportunities for experimentation and innovation, while also maintaining a fair market and a healthy economy, as well as protecting society.

The practice of law itself is already being impacted by AI to various degrees, but clearly there are several potentially significant additional functions and benefits to lawyers and their clients that might be secured. It seems likely that if firms have not already started considering how AI might enhance their practice, they will likely do so soon.

For the time being, the use of AI in Australia will continue to be governed by existing legislation, such as privacy laws, consumer laws, the Online Safety Act, IP and cybersecurity, to name a few (and the voluntary AI Ethics Principles). As the roll out of AI continues to gain momentum, there may be a need for AI-specific regulation both in Australia and globally.

The current expectation is that most regulatory frameworks (globally) will be based on the EU AI Act and/or the Canadian Directive of Automated Decision Making , which are considered to be two of the most advanced and comprehensive frameworks in existence and appear to have set the precedent for any future regulation. Keeping track of developments is an important task for businesses that operate in multiple jurisdictions. As different jurisdictions have varying appetites for risk, the result will likely be a patchwork of regulatory frameworks and guidelines that businesses need to navigate carefully.

As the AI era continues to evolve, our firm will continue to monitor this developing area of risk and regulation. We have several legal experts who are closely monitoring developments globally in relation to policy, law and technology, and are prepared to support your business through the challenges which lie ahead, to make fast and effective decisions, and to successfully implement AI into your business.

Do Not Just Take Our Word for It

"The team are responsive to our needs and provide strategic advice to achieve rapid resolution."

The Legal 500 Asia Pacific

"Squire Patton Boggs lawyers are strong across the board in the critical areas for providing excellent legal advice and representation in general litigation. Their lawyers are all clever, highly motivated, hardworking and easy to get along with. They work very well as a team, successfully calling upon the skills and experience of all involved. They remain client and outcome focused at all times."

The Legal 500 Asia Pacific

"I felt very confident having Squire Patton Boggs on our team."

The Legal 500 Asia Pacific

"Partner availability, involvement and accessibility is exceptionally good."

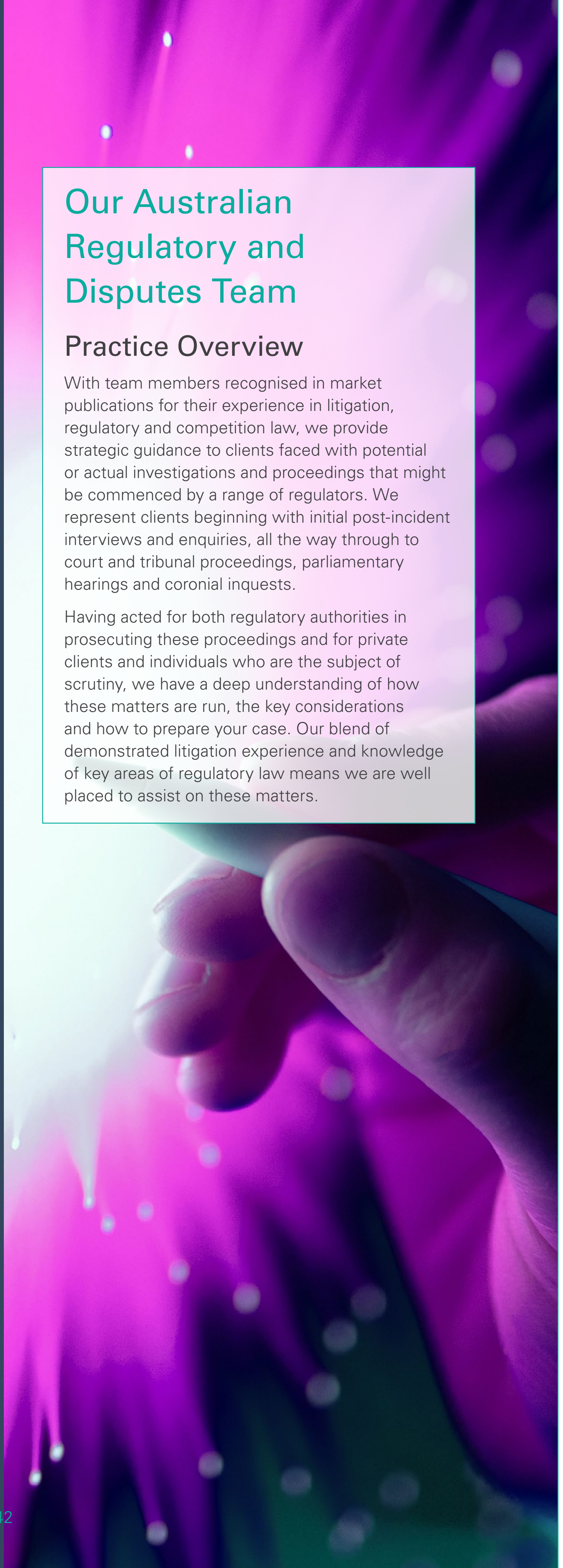
The Legal 500 Asia Pacific

"The team at Squire Patton Boggs are constantly working to develop novel solutions to very complex and commercial issues."

Founder and CEO of a global company

"I need advisors that not only have the legal expertise, but also the commercial know-how and industry-specific knowledge to achieve my business outcomes and, in my opinion, the Squire Patton Boggs team has the perfect blend of these attributes."

Executive chairman, ASX-listed company



Our Australian Regulatory and Disputes Team

Practice Overview

With team members recognised in market publications for their experience in litigation, regulatory and competition law, we provide strategic guidance to clients faced with potential or actual investigations and proceedings that might be commenced by a range of regulators. We represent clients beginning with initial post-incident interviews and enquiries, all the way through to court and tribunal proceedings, parliamentary hearings and coronial inquests.

Having acted for both regulatory authorities in prosecuting these proceedings and for private clients and individuals who are the subject of scrutiny, we have a deep understanding of how these matters are run, the key considerations and how to prepare your case. Our blend of demonstrated litigation experience and knowledge of key areas of regulatory law means we are well placed to assist on these matters.

Key Contacts

Australia

Graeme Slattery
Partner, Sydney
T +61 2 8248 7876
E graeme.slattery@squirepb.com

David Starkoff
Partner, Sydney
T +61 2 8248 7833
E david.starkoff@squirepb.com

Rebecca Heath
Partner, Perth
T +61 8 9429 7476
E rebecca.heath@squirepb.com

Angela Radich
Director, Sydney
T +61 2 8248 7874
E angela.radich@squirepb.com

David Skender
Director, Perth
T david.skender@squirepb.com
E +61 8 9429 7434

Emma Salkavich
Senior Associate, Sydney
T +61 2 8248 7861
E emma.salkavich@squirepb.com

Jessica Tomlinson
Senior Associate, Perth
T +61 8 9429 7403
E jessica.tomlinson@squirepb.com

Jon Baker
Senior Associate, Perth
T +61 8 9429 7618
E jon.baker@squirepb.com

Tom Haystead
Senior Associate, Sydney
T +61 2 8248 7807
E tom.haystead@squirepb.com

Connor McClymont
Senior Associate, Perth
T +61 8 9429 7534
E connor.mcclymont@squirepb.com

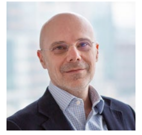
Global

Alan Friel
Global Chair, Data Privacy, Cybersecurity & Digital Assets, Los Angeles
T +1 213 689 6518
E alan.friel@squirepb.com

Charles Helleputte
Partner, Data Privacy, Cybersecurity & Digital Assets, Brussels
T +32 2 627 1100
E charles.helleputte@squirepb.com

Charmian Aw
Partner, Data Privacy, Cybersecurity & Digital Assets, Singapore
T +65 6922 8679
E charmian.aw@squirepb.com

Julia Jacobson
Partner, Data Privacy, Cybersecurity & Digital Assets, New York
T +1 212 872 9832
E julia.jacobson@squirepb.com



David Naylor
Partner, Data Privacy, Cybersecurity & Digital Assets, London
T +44 20 7655 1668
E david.naylor@squirepb.com

Malcolm Dowden
Co-head of Knowledge Management, Data Privacy, Cybersecurity & Digital Assets, London
T +44 20 7655 1665
E malcolm.dowden@squirepb.com

SQUIRE
PATTON BOGGS

squirepattonboggs.com