THE LAW SOCIETY
OF NEW SOUTH WALES

Our ref: PDL/PuLC:BMsb080524

8 May 2024

Dr James Popple
Chief Executive Officer
Law Council of Australia
PO Box 5350
Braddon ACT 2612

By email: john.farrell@lawcouncil.au

Dear Dr Popple,

Opportunities and impacts arising out of the uptake of artificial intelligence (AI) technologies in Australia

The Law Society is grateful for the opportunity to contribute to the Law Council's submission to the Senate Select Committee on Adopting Artificial Intelligence, in response to its inquiry into the opportunities and impacts arising out of the uptake of artificial intelligence (**AI**) technologies in Australia. The Law Society's Privacy and Data Law and Public Law Committees have contributed to this submission.

Consistent with previous Commonwealth consultations on AI, the terms of reference of this inquiry are drawn broadly. This breadth acknowledges the scale of transformation occurring with the accelerated development and deployment of AI. Significant work is also being undertaken internationally to protect against emerging risks posed by AI while at the same time creating the conditions which will allow for the significant economic and other benefits and opportunities arising from the technologies.

As set out in our submission to the Law Council dated 17 July 2023 (**2023 submission**), the Law Society supports the development of safe and responsible AI in Australia through an interoperable framework that promotes innovation while maintaining appropriate safeguards.[1] In particular, we support a focus on transparency, accountability, contestability and responsibility. As AI is a contextual term that is used to refer to a broad spectrum of computer science developments from around the 1950s onwards, we suggest there is benefit in developing a common understanding of the characteristics of AI that require regulation, rather than targeting one system or iteration of the technologies.

At the outset, we note that there are several reviews and other work occurring across government, both at the Commonwealth and State levels, that is relevant to the deployment and regulation of AI in Australia.

[1] Law Society of New South Wales, Safe and responsible AI in Australia (Submission, 17 July 2023).

For example,

- The Review of the *Privacy Act 1988* (Cth) has been completed, with the Government response released on 28 September 2023;[2]
- The Department of Industry, Science and Resources' consultation, 'Safe and responsible AI in Australia' has closed, with an interim response by the Government published on 17 January 2024;[3]
- Ongoing work of the AI in Government Taskforce;[4]
- Ongoing work of the Data and Digital Ministers Meeting;[5]
- Ongoing work of the Office of the ESafety Commissioner, including new mandatory industry codes and the development of two mandatory industry standards to deal with illegal and harmful content;[6] and
- Ongoing work on cybersecurity through the Cyber Security Strategy.[7]

This work across government is reflective of the range of opportunities and risks posed by AI, as well as the pace of progress. We consider that it is important to ensure that government inquiries/working groups at both Commonwealth and State levels speak to each other and avoid unnecessary duplication of work on this issue. Any framework in Australia to regulate AI must be coordinated, even if there is no single regulatory function tasked to govern AI. Many of the issues arising in this area are cross-cutting and coordination will help to reduce uncertainty for business, as well as fostering the right climate for innovation and investment.

As noted below, developments in AI governance are occurring in key jurisdictions around the world. It is important for the Government to leverage this work, including by collaborating with international partners on interoperable measures to support safe and responsible AI. At the same time, harmonised laws within Australia itself and a coordinated approach at the Commonwealth and State levels will be a key measure of success.

We make brief comments in response to Terms of Reference (b), (c), (e) and (f) below:

(b) Risks and harms arising from the adoption of technologies, including bias, discrimination and error

There are foreseeable risks and harms arising from the adoption of AI, as well as risks that may only come to light as the technologies mature or develop, and as new technologies enter the market. Many risks have already been extensively documented, and can be categorised in terms of the technical risks, the human rights/societal risks, and what has been described as the 'existential risks…arising out of concerns of what it means to be human and how…we understand human machine interactions'.[8]

The Commonwealth Government has already begun through inquiries, such as the Safe and Responsible AI in Australia consultation, to identify the technical risks of AI. These include inaccuracies in model inputs and outputs; biased or poor-quality model training data; model

[2] Attorney General's Department, Review of the Privacy Act 1988 (Webpage), including Government response to the Privacy Act Review Report available here.
[3] Department of Industry and Resources, Supporting responsible AI: discussion paper (Webpage), with Government's interim response available here.
[4] Australian Government, Digital Transformation Agency, The AI in Government Taskforce: examining use and governance of AI by the APS (Media Release, 20 September 2023).
[5] Department of Finance, Data and Digital Ministers Meeting (Webpage).
[6] Office of the ESafety Commissioner, 'Search engines will need to take steps to tackle child sexual abuse material and AI misuse under new code' (Media release, 12 March 2024).
[7] Department of Home Affairs, '2023-2030 Australian Cyber Security Strategy' (Webpage).
[8] See School of Computing and Information Systems and Centre for Artificial Intelligence & Digital Ethics, University of Melbourne, Submission to the Safe and Responsible AI in Australia consultation (Submission, August 2023).

slippage over time; discriminatory or biased outputs and a lack of transparency around the use of AI.[9] Particular emphasis has been placed on the 'frontier' models of AI, namely highly capable, general-purpose AI models, particularly those being developed outside of Australia.

It is equally important to look at the way in which the technical risks interact with the various possible applications of AI technologies, leading to human rights and societal risks. While we are not equipped to provide a comprehensive overview of high-risk settings here, in our view, Australia should leverage existing work of other jurisdictions that have employed a risk-based approach to AI regulation. As discussed below, the European Union's (**EU**) AI Act engages a tiered system, with many of the identified risks also applicable to the Australian context.

Under the EU AI Act, banned uses are enumerated.[10] These include, for example, social scoring; assessing the risk of an individual committing criminal offences solely based on profiling or personality traits; 'real-time' remote biometric identification in publicly accessible spaces for law enforcement; biometric categorisation systems inferring sensitive attributes; and compiling facial recognition databases.

A fairly complex assessment is required under the EU AI Act to identify High Risk AI Systems, with the determination depending on whether the AI system is used as a component of certain products set out in Annex II (e.g., medical devices, cableway installation); or if the system performs functions set out in Annex III (e.g., certain biometric purposes, critical infrastructure, law enforcement, migration and asylum management, educational and vocational training and judicial or democratic processes).

While we do not consider that a single statute on AI such as has been adopted in the European Union is appropriate for the Australian context, the Government can certainly draw on the detailed work and thinking in that jurisdiction around levels of risk, and the adoption of a risk-based approach to regulation of AI. Identification of high-risk settings can facilitate further discussion on the additional guardrails and the extent of regulatory intervention required to reduce the likelihood of harm, whether through existing, technology-neutral frameworks (e.g., privacy laws, healthcare, anti-discrimination, and financial sector laws) or, in specific cases, through dedicated legislation.

The risks associated with a lack of transparency are of particular concern. As summarised in the Government's response to the Safe and Responsible Use Consultation:

> opaque AI systems can make it difficult to identify harms, predict sources of error, establish accountability, explain model outcomes and assure quality. For example, if job applications are assessed by 'black box' AI systems (where internal workings are automated and invisible), people affected by discriminatory outcomes may have limited ability to understand or question decisions.[11]

From an administrative law perspective, these issues are significant, considering the increasing reach of governments into citizens' lives, coupled with a greater reliance on algorithmic systems in aiding the process of government decision-making. These risks are not mitigated simply by the subject of the decision being informed that AI was used. Rather, effective mitigation also requires meaningful and intelligible explanation on how the AI was deployed. This should include disclosure of the data sets on which it was trained, how the inputs are made into outputs, the rules on which the system operates, how biases have been mitigated, and other details relevant to the circumstances. In this context, we commend the

[9] Australian Government, Safe and responsible AI in Australia consultation – Interim Response (17 January 2024).
[10] https://artificialintelligenceact.eu/article/5/ See EU AI Act, Chapter II: Prohibited Artificial Intelligence Practices, Article 5.
[11] See above (n 9) 11.

work already undertaken in NSW, for example, the NSW Ombudsman's report of 2021, which focused on the use of AI and automated decision-making systems by public sector agencies, including with reference to core administrative law principles such as procedural fairness.[12]

Numerous decisions are made every day by public officers that involve the exercise of discretion. Decision-makers must engage in an active intellectual process in making such decisions.[13] Protections need to be considered and developed lest this process become automated and box-ticking in nature. It is the active consideration of individual circumstances that underpins much of the character of the common law and statutory protections against the misuse of executive power.

In the absence of a comprehensive, human rights-based framework at the Commonwealth level, there needs to be a principled approach to mitigate risks, such as bias in the input data, automatic bias and algorithmic bias, particularly the impacts on the human rights of vulnerable populations, as well as intrusions on the right to privacy. As noted in our 2023 submission, framing these considerations through the lens of harm minimisation (i.e., considering the potential harms to humans and regulating accordingly) is one way to assist this process.

(c) Emerging international approaches to mitigating AI risks

Different regulatory approaches are being developed internationally to mitigate the risks of AI in what has been described by some commentators as a 'race' where 'incentives, standards and hard regulation are intertwined with geopolitical, technological and value-driven interests'.[14]

The Law Council, in its submission to the Department of Industry, Science and Resources, cautioned against the adoption of any particular regulatory model in Australia at this stage, noting:

> Australia has an opportunity to assess the regulatory models adopted by other jurisdictions and to determine an optimal and bespoke approach for Australia that reflects the nuances of Australia's pre-existing constitutional and regulatory framework, and different local market environment.[15]

The Law Society agrees that any framework in Australia should be adapted to pre-existing regulatory processes, as well as our economic and social conditions and legal culture. The challenge facing Australia is to seek a degree of alignment with jurisdictions with whom we share the values of transparency, accountability and explainability of AI technologies, while allowing sufficient flexibility for innovation so that Australian organisations are able to adopt AI, as well as develop and create AI products.

The importance of interoperability

The Law Society supports an Australian framework that promotes interoperability with international AI governance regimes. From an economic perspective, this is important to ensure that Australia attracts business from innovators and investors in AI technologies. The

[12] New South Wales Ombudsman, 'The new machinery of government: Using machine technology in administrative decision-making' (Report, 29 November 2021). See also New South Wales Ombudsman, 'A map of automated decision-making in the NSW Public Sector') (Report, 8 March 2024).
[13] See, for example, *Minister for Immigration, Citizenship and Multicultural Affairs v McQueen* [2024] HCA 11 at [6].
[14] United States Study Centre, 'Standardisation, trust and democratic principles: The global race to regulate artificial intelligence' (Report, 31 July 2023).
[15] Law Council of Australia, Submission to the Safe and Responsible AI in Australia consultation (17 August 2023).

framework must be adaptable and flexible to allow for change, and subject to relatively frequent review to ensure relevant legislation and its administration and enforcement remain fit for purpose. Harmonised State and Commonwealth laws, as well as interoperability with international regimes, will help create the right climate for trade and investment.

Given that AI supply chains often occur across borders, Australia should be engaging through bilateral and multilateral channels to influence other jurisdictions' approach to the regulation of AI in a way that aligns with our values, including democracy, the rule of law and respect for human rights.

Approach in key jurisdictions – Recent developments

- *United Kingdom*

The UK's Department for Science, Innovation and Technology and its Office for Artificial Intelligence published a white paper setting out a pro-innovation approach to AI regulation on 29 March 2023 (**AI White Paper**).[16] In short, the key recommendation of the White Paper was that the UK government should introduce principle-based regulation, with implementation to occur through existing regulators, but with central coordination to ensure proper oversight and to address cross-cutting risks.

The AI Framework, which draws on the principles for ethical AI use, defined by the OECD, emphasises the following:

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

The principles are not designed to be put on a statutory footing, but rather will be implemented by existing regulators, so as to draw on their domain-specific expertise.

The UK Government's response to the AI White Paper was published on 6 February 2024.[17] The emphasis continues to be on voluntary measures directed to AI developers, which in the future may require the enactment of relevant legislation once the understanding of risk has matured. Regulators have also been tasked with incorporating the principles into their work in a transparent way and were required to publish an outline of their strategic approach by 30 April 2024.

The UK Government's next steps in 2024 include working with regulators on AI regulatory policy; undertaking a gap analysis in existing regulatory powers and remits; developing a central function to drive coherence in the regulatory approach; providing guidance and support for AI adoption across industries; and supporting international collaboration on AI governance.[18]

At the same time, we note that in November 2023, a Private Members Bill was introduced into the House of Lords which seeks to establish the creation of an AI Authority to oversee the

[16] Department for Science, Innovation and Technology and Office for Artificial Intelligence, 'AI regulation: a pro-innovation approach'(29 March 2023).
[17] UK Government, 'A pro-innovation approach to AI regulation: government response' (6 February 2024).
[18] Ibid.

regulatory framework. The second reading occurred on 22 March 2024 and the Bill is now at the third reading stage.[19]

- *European Union*

The EU AI Act was adopted by the European Parliament on 13 March 2024. It is anticipated that the Act will be formally adopted by the Council of the EU by the end of May 2024, will enter into force incrementally from 20 days after its publication in the Official Journal, and will be fully applicable two years later, with some exceptions.

The Act is the first comprehensive regulatory framework with respect to the development and use of AI. It adopts a functional risk-based approach. Certain categories of AI systems (e.g., social scoring systems) are considered an unacceptable risk and banned outright. The greatest regulation then applies to systems which are considered to create a high risk to the health and safety, or fundamental rights, of European citizens. These systems must meet requirements such as the establishment, implementation, documentation and maintenance of a risk management system, data governance and management practices, technical documentation, record logs, information for deployers, cybersecurity and human oversight.

In addition, there are rules for general-purpose AI systems (**GPAIs**) which seek to ensure transparency along the value chain, including requirements to compile technical information, comply with copyright rules, and publish summaries of the data used to train the model.[20]

The territorial application of the legislation is broad in that it will apply to operators who supply AI and GPAI models to the EU market, as well as to organisations that use AI systems for business purposes that are located or established in the EU, or if the output from the AI system is used in the EU.

- *United States*

In October 2023, US President Joe Biden released an Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence (EO).[21] In contrast to the EU AI Act, which has a focus on enforcement of regulations with significant fines for non-compliance, the EO is focused on guidelines and regulation.

There are certain commonalties of approach, however, in both the EU AI Act and the EO, including testing and monitoring across the lifecycle of the AI system, an emphasis on post-market/post-deployment monitoring, privacy law, and adherence to cybersecurity standards.[22]

Action that has been taken since the EO in relation to managing risks to safety and security includes requiring the most powerful AI systems to report vital information, such as safety test results, to the Department of Commerce, conducting risk analysis of AI's use in every critical infrastructure sector, and a draft rule that requires reporting by US cloud companies who provide computing power for foreign AI training.[23]

---

[19] See Artificial Intelligence (Regulation) Private Members Bill [House of Lords] (22 November 2023).
[20] See further information in the High-level summary of the AI Act (27 February 2024), with full text of the Act available here.
[21] White House, Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (30 October 2023).
[22] See DLA Piper, 'Comparing the US AI Executive Order and the EU AI Act' (7 December 2023).
[23] The White House, 'Fact Sheet: Biden-Harris Administration Announces Key AI Actions Following President Biden's Landmark Executive Order' (29 January 2024).

(e) Opportunities to foster a responsible AI industry in Australia

As set out in our 2023 submission, we are of the view that a framework that is flexible and scalable to future technological change will allow for sufficient innovation while maintaining appropriate guardrails. Any approach should focus on the particular characteristics and functional capabilities of the technologies that demand a regulatory response (e.g., their adaptivity and autonomy) rather than strict rules for particular new iterations e.g. , Gen AI.[24]

Any framework should be coherent with Australia's other regulatory regimes and, to the extent possible, be interoperable with other frameworks that have been developed globally (see above). This framework should be underpinned by ethical principles and standards that are applicable across the AI life cycle, from design, training and testing, to provision of a service/good to the end-user. Such principles include a focus on transparency (i.e., signalling when and how AI has been used), accountability (i.e., ensuring that there are systems in place to oversee design, development, deployment and operation of the technologies), and contestability (i.e., the ability to fairly challenge a decision made by AI).

In light of the rapid developments in AI, any framework, regulatory or otherwise, should be subject to shorter, accelerated review cycles than would normally apply. We support a risk-management approach which focuses on having adequate systems in place to monitor and detect adverse consequences when they do arise.

A 'detect and respond' model can reduce the need for upfront restriction or prohibition. It is appropriate that regulated entities are required to apply a 'risk of harms' assessment appropriate to mitigate risk, but this should be done in a way that avoids prescriptive rules which are likely to be ill-fitted to the pace of technological development in this field.

(f) Potential threats to democracy and trust in institutions from generative AI

There are various circumstances whereby AI, combined with key datasets or 'Big Data', may pose a potential threat to democracy and trust in institutions.

In terms of the electoral process itself, all jurisdictions will need to adopt measures to address unlawful interference, whether by foreign or domestic actors, in electoral processes. At the same time, there is a need to ensure that the use of AI to target voters occurs with adequate safeguards and transparency.

The risk of AI tainting the electoral process is not theoretical: the use of deepfakes has been observed in recent elections in Argentina and Slovakia.[25] In recent days, Meta AI has also taken the step of blocking queries on political candidates and election-related content on its chatbot in India.[26] While AI platforms themselves are self-regulating to some extent, for example requiring advertisers to disclose the use of AI to alter an advertisement on a political or social issue, the Australian Government should carefully consider whether electoral legislation adequately guards against the risks posed by AI while still allowing for freedom of political communication.[27]

We note that the Joint Standing Committee on Electoral Matters, as a result of its inquiry into the Conduct of the 2022 Federal Election, recommended that the Australian Government

[24] Note that this approach was promulgated in the UK's recent White Paper. See above n 17.
[25] Brian Wheeler and Gordon Corera (BBC), 'Fears UK not ready for deepfake general election' (21 December 2023); Jack Nicas and Lucía Cholakian Herrera (New York Times), 'Is Argentina the First A.I. Election?' (15 November 2023).
[26] Pranshu Verma and Cat Zakrzewski (The Washington Post), 'AI deepfakes threaten to upend global elections. No one can stop them' (23 April 2024).
[27] See Statement from Meta, 'How Meta Is Planning for Elections in 2024' (28 November 2023).

develop legislation, or seek to amend the *Commonwealth Electoral Act 1918* (Cth), to provide for the introduction of measures to govern truth in political advertising, giving consideration to provisions in the *Electoral Act 1985* (SA).[28] We support the introduction of such legislation and emphasise the need for meaningful consultation and careful drafting to maximise its effectiveness, including to ensure relevant use of AI is captured.

In terms of democratic culture itself, we note the potential for serious and wide-spread harm arising from AI-generated misinformation and disinformation disseminated on online platforms. We support the position adopted by the Law Council, namely in-principle support for appropriate and proportionate regulation that enables individuals and organisations to identify and address this material.[29]

Commentators from the Brookings Institute have foreshadowed a further risk to democratic culture through the 'increasingly centralised control' of AI, considering that 'just three Big Tech firms (Microsoft, Google and Amazon) control two-thirds of the global market for cloud computing resources used to develop AI models'.[30] They have suggested that governments should not simply regulate, but also implement so-called 'Public AI' systems, noting:

> Publicly developed and owned AI models and computing infrastructure could democratize the technology itself, creating an open platform for innovation and offering guarantees about the availability, equitability, and sustainability of AI technology.[31]

These suggestions obviously rely on strengthening the digital capacity of government through significant investment in AI research and development. We are already seeing this type of investment in other jurisdictions, for example the recent announcement in the UK of £900m towards an exascale computer for the training of AI models to be deployed across science, industry and defence.[32]

Thank you for the opportunity to contribute. Questions at first instance may be directed to Sophie Bathurst, Policy Lawyer, at (02) 9926 0285 or Sophie.Bathurst@lawsociety.com.au.

Yours sincerely,

Brett McGrath
President

[28] Inquiry into the 2022 Federal Election – Parliament of Australia (Recommendation 11 of the Interim Report).
[29] Law Council of Australia, Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2023— Exposure Draft (29 August 2023).
[30] Nathan Sanders, Bruce Schneier, and Norman Eisen, 'How public AI can strengthen democracy' (4 March 2024).
[31] Ibid.
[32] Dan Milmo and Alex Hern (The Guardian), 'UK to invest £900m in supercomputer in bid to build own 'BritGPT'' (16 March 2023).