Queensland Law Society

Law Society House, 179 Ann Street, Brisbane Qld 4000, Australia
GPO Box 1785, Brisbane Qld 4001 | ABN 33 423 389 441
P 07 3842 5943 | F 07 3221 9329 | president@qls.com.au | qls.com.au
Office of the President

19 July 2023

Our ref: [MC:LP]

Dr James Popple
Chief Executive Officer
Law Council of Australia
19 Torrens St
Braddon ACT 2612

By email: [redacted]

Dear Dr Popple

Safe and responsible AI in Australia

Thank you for the opportunity for the Queensland Law Society (**QLS**) to provide feedback to inform the Law Council's response to the Department of Industry, Science and Resources' Discussion Paper, 'Safe and responsible AI in Australia' (**the Discussion Paper**).

This response has been compiled with input from the QLS Privacy, Data, Technology and Intellectual Property Committee, Competition and Consumer Law Committee and the Innovation Committee, whose members have substantial expertise in this area.

Introductory comments

QLS strongly supports enhanced regulatory and governance initiatives to ensure artificial intelligence (**AI**) is developed and used safely in both the public and private sectors.

Various inquiries have identified that there are a number of areas in which the existing Australian legal framework is deficient in responding to the risks offered by AI.[1] QLS has previously submitted that there are already inconsistencies that exist within the existing legal framework with the delegation to computerised decision-making.[2] We agree with the Law Council's submission to the 2022 Issues Paper that there is need for harmonising reform[3] in this area in conjunction with additional regulatory and governance responses to AI regulation.

---

[1] The QLS submission to the Law Council dated 10 May 2022 in response to the 'Positioning Australia as a leader in Digital Economy Regulation – Automated Decision Making and AI Regulation – Issues Paper' also outlined a number of areas requiring review.
[2] Angus Murray, '*Legal technology: Computer says no ...but then what*' (2019) 39(8) Proctor, 48-49.
[3] Law Council of Australia, Submission to Digital Technology Taskforce, Department of the Prime Minister and

Whilst jurisdictions have been cautious to avoid adopting 'a heavy-handed' approach to AI regulation which stifles innovation,[4] analogous approaches taken with respect to the development of social media platforms and protection of privacy suggest that a precautionary approach ought to be applied. This is particularly important in the context of an ill-defined and rapid evolving technology, the parameters of which are unknown.

Citizens are already at a significant informational disadvantage in terms of AI-related systems, AI-related data and associated infrastructure access and most often, lack the resources to challenge alleged AI abuses including automated decision-making. The Robodebt failure also clearly emphasised the importance of transparency and AI-creator/user accountability to civil society in a context of increased adoption of automated decision-making and the training and use of AI related technologies more broadly.

Against this background, QLS supports a multifaceted risk-based approach to AI regulation which encompasses prohibitions (with clearly articulated exceptions) and mandatory standards for both the development and use of AI. Regulatory responses should reflect the market dominance of owners of existing AI service offerings and reflect the precautionary principle[5] in terms of AI products. They should also ensure that regulation which impacts smaller organisations is meaningful and proportionate. The key principles to inform the regulation being transparency, fairness, accountability, privacy, security and safety for consumers and the public who may be at risk of harm.

QLS recommends the LCA emphasise that regulatory mechanisms should reflect and entrench Australia's AI Ethics Framework.[6] The LCA should also emphasise Australia's adherence to the OECD AI Principles[7] which provides, amongst others, the following principles for 'responsible stewardship of trustworthy AI':

> *1.2. Human-centred values and fairness*
>
> *a) AI actors should respect the rule of law, human rights and democratic values, throughout the AI system lifecycle. These include freedom, dignity and autonomy, privacy and data protection, non-discrimination and equality, diversity, fairness, social justice, and internationally recognised labour rights.*

Cabinet *Positioning Australia as a leader in digital economy regulation – Automated decision making and AI regulation* (3 June 2022).

[4] Department for Science, Innovation & Technology, United Kingdom Government, *A pro-innovation approach to AI regulation* (Policy paper No. 815, 29 March 2023) <https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper>

[5] Didier Bourguignon, *The Precautionary Principle – Definitions, applications and governance,* European Parliament In-Depth Analysis (PE 573.876 December 2015).

[6] Department of Industry, Science and Resources, Australia's Artificial Intelligence Ethic Framework', *Australian Government – Department of Industry, Science and Resources* (Web Page, 7 November 2019) <https://www.industry.gov.au/publications/australias-artificial-intelligence-ethics-framework#:~:text=The%20Artificial%20Intelligence%20%28AI%29%20Ethics%20Framework%20guides%20businesses,a%20global%20leader%20in%20responsible%20and%20inclusive%20AI.>

[7] Organisation for Economic Co-operation and Development, 'Recommendation of the Council of Artificial Intelligence', *OECD Legal Instruments* (Recommendation, 22 May 2019) <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449#adherents>

b) *To this end, AI actors should implement mechanisms and safeguards, such as capacity for human determination, that are appropriate to the context and consistent with the state of art.*

QLS notes that the scope of the current Discussion Paper seeks to identify potential gaps in the domestic governance landscape and any possible additional AI governance mechanisms to support the development and adoption of AI. We observe that Australia's current approach relies on general regulations, sector specific regulation and voluntary or self-regulation initiatives.

What further governance and regulatory responses are needed?

As outlined above, QLS supports a strengthened regulatory response based upon the precautionary principle[8] to manage the potential risks of AI.

In considering what additional responses are required, QLS notes there is a divergence in regulatory approaches between current "soft law" approaches and the "hard law" direction of the European Union with its proposed AI Act.[9]

Proponents of a soft law approach recognise that AI is still new technology and it is unclear how it is going to develop and the risks its use may pose. Whilst a soft law approach provides flexibility to respond, limitations created by flexibility are increased risk, greater uncertainty, reduced transparency and insufficient accountability.[10] In our view, the significant risks posed by the use of AI justifies a strengthened and precautionary approach to AI regulation.

We note the Discussion Paper builds on the recent rapid research report on generative AI by Australia's National Science and Technology Council. That report observed there 'is a growing recognition that a range of institutional measures and policies are likely to be required to mitigate public risks. However, risk management approaches are most effective within a specific context of use, and against technical rather than social or systemic risks, such as use by social media platforms.'[11]

As such, QLS supports a multifaceted approach to AI regulation. Governance responses should encompass precautionary-principle and risk-based regulatory approaches, specific sector and use prohibitions (for unacceptable risks) and mandatory standards, consistent with the direction being taken by the EU.

---

[8] Bourguignon (n. 5).

[9] European Parliament, *Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts*, Doc No.: (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD), 14 June 2023'.

[10] Leslie, D., Burr, C., Aitken, M., Cowls, J., Katell, M., and Briggs, M. (2021). Artificial intelligence, human rights, democracy, and the rule of law: a primer. The Council of Europe. < https://rm.coe.int/primer-en-new-cover-pages-coe-english-compressed-2754-7186-0228-v-1/1680a2fd4a> at p 26.

[11] Bell, G., Burgess, J., Thomas, J., and Sadiq, S. (2023, March 24). Rapid Response Information Report: Generative AI - language models (LLMs) and multimodal foundation models (MFMs). Australian Council of Learned Academies <https://www.chiefscientist.gov.au/sites/default/files/2023-06/Rapid%20Response%20Information%20Report%20-%20Generative%20AI%20v1_1.pdf> p 15.

International best practice.

QLS considers that the two best risk regulatory frameworks currently available as a template for Australia are those reflected in the EU's AI Act[12] and the US National Institute of Standards and Technology 'AI Risk Management Framework (version 1.0)' (**the NIST risk framework**).[13]

The AI Act is premised on a four category risk classification system and accompanying risk-based regulations and standards.[14] The advantage of the European approach is a clear articulation of which uses of AI pose the greatest risk with a consequent regulatory focus on those areas. Although opinions will differ as to the relative risk of certain applications, the reality is that use of AI will vary from the trivial to the critical, and a one-size-fits-all approach is not viable.

The NIST risk framework provides actionable insights and is well suited to practical implementation in a wide range of projects. Whilst the regulatory framework applied to a fast evolving area of technology should not attempt to be too granular, the primary objective of the NIST risk framework is likely to remain current for at least the current generation of AI tools.

We acknowledge that the nature of risk in the development and use of AI is a sliding scale and that risk frameworks are likely to evolve over time.[15] It is also unclear whether the proposed AI Act for example will respond to "general purpose" AI applications such as ChatGPT.[16]

We suggest that the LCA should reiterate the need for regulatory collaboration/information sharing and consultation with various legal, technical and other stakeholders to ensure that AI frameworks can identify and respond to risks as they emerge.

It may be that a dedicated oversight body will be required to properly coordinate and administer international findings and development, as well as the risks and evolution of AI from a regulatory perspective.

Whilst the uptake of AI applications across the vast range of public and private sector undertakings which affect most individuals and business in some way is nascent, AI technologies are rapidly evolving. As such, the applicable regulations and standards need to be sufficiently flexible to respond to developments in technology, use cases and new (or changing) risks. Regulatory responses should take into account existing sector specific requirements (as well as risks and use cases) and ensure that obligations are easily understood and proportionate. Clearly articulated principles together with regulatory guidance (as opposed to prescriptive requirements), can be a helpful way of enabling regulation to be sufficiently flexible to respond to changing technology and community expectations with respect to the development and use of AI by the public and private sectors.

---

[12] Tambiama Madiega, 'Artificial intelligence act', *European Parliamentary Research Service* (Briefing, June 2023) <https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf>.

[13] Gina M. Raimondo and Laurie E. Locascio, 'Artificial Intelligence Risk Management Framework (AI RMF 1.0)' *National Institute of Standards and Technology* (Framework, January 2023) < https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf>.

[14] 'The European Union's Artificial Intelligence Act – explained' *world Economic Forum* (Web Page, 30 June 2023) <https://www.weforum.org/agenda/2023/06/european-union-ai-act-explained/>

[15] William Crumpler, 'Europe's Strategy for AI Regulation' *Centre for Strategic and International Studies* (Blog Post, 21 February 2020) <https://www.csis.org/blogs/strategic-technologies-blog/europes-strategy-ai-regulation>.

[16] *Bell, Burgess, Thomas and Sadiq* (n. 9) 15, Appendix 3.

As a baseline and consistent with Australia's AI Ethics Principles, organisations that use or engage with an AI-related service should be required to disclose details about the nature of its use and engagement within an AI policy statement. To overcome the limitations observed in the privacy disclosure system, consideration should also be given to formalising any policy statement in a prescribed plain language and consumer directed form.

Supporting compliance by small to medium enterprises

Our members acknowledge that, depending on the regulatory approach, introducing regulation of AI could stifle innovation, particularly for small to medium enterprises (**SMEs**). It will be important to ensure any regulatory approach avoid duplication, is consistent and proportionate, and provides clear guidance and support for compliance to SMEs.

QLS supports education and other tools to encourage and facilitate compliance. In our view, organisations and industry should be supported to assess the risks to individuals and the impact on their fundamental rights which may result from AI use. This would be in addition to education around existing legal frameworks that apply to the development and use of AI, including with respect to privacy and consumer protection. Thought should also be given to the key actors in AI applications having responsibility to assist in relevant assessments by small business.

Examples of tools to support positive business practices from the National AI Centre and Singapore are outlined in the Discussion Paper[17] and could also include guidance and practical tools such as the model contractual clauses published by the European Commission for data transfers between EU and non-EU countries.

QLS further supports more general education for the public with respect to AI.

Other areas for consideration

AI and automated decision-making

QLS acknowledges the stated focus of the paper is 'AI' but where relevant it draws linkages to related applications such as automated decision-making (**ADM**). We note that even in circumstances where ADM has not used AI technologies, the risks associated with ADM may be reduced by some of the governance responses proposed in the Discussion Paper.[18]

In preparing our response, QLS has had regard to the recently published Report of the Royal Commission into the Robodebt Scheme, presented by Commissioner Holmes AC SC (**the Robodebt report**) on 7 July 2023.

In particular we highlight the following:

- the Commissioner's consideration that there should be independent oversight in respect of government automated decision-making; [19]

[17] Safe and responsible AI in Australia, Discussion Paper, pp 15 and 22.
[18] Safe and responsible AI in Australia, Discussion Paper, p 6.
[19] Catherine Holmes AC SC, *Royal Commission into the Robodebt Scheme* (Final Report, Volume 1, 7 July 2023), 485.

- in respect of system design, the Commissioner stated:

  The software used in any such system must not only ensure accuracy, but also ensure that persons subject to decisions made by an automated process can know or understand the reasons behind those decisions. A clear path for review of decisions is important in designing a system which adheres to the OECD AI principles: "a person affected by a decision should understand why the decision was made, and there should be pathways for review of these decisions that are accessible to them"; [20] and

- recommendation 17.1 in respect of recommended reform to the legal framework in which automation in government services can operate.

Whilst not exhaustive, **Attachment A** also sets out some of the issues highlighted by the Robodebt inquiry. The Government's response to the Robodebt report must also be considered in the context of AI regulatory responses.

Biometrics and responding to 'deep fakes'

In addition to ADM, our members have also identified the risks posed by AI-generated media including deep fakes and uses in political and other contexts, and also AI related technologies including the use of biometrics.

Some of our members have queried the extent to which existing legal frameworks respond to generative deep fakes in a manner which adequately protects individual identity (and provides a means of redress for individuals) and potential options for reform in this area. The use of these in an electoral context is also a serious issue as to online misinformation and disinformation.

The collection and use of biometric information (such as that obtained in facial recognition technology) also poses significant privacy implications. We note consideration of this issue forms part of the Government's current Privacy Act Review. Proposals to use biometrics for establishment and verification of identity (with consent)[21] reiterate the need to prioritise and coherently integrate AI and privacy and related reforms to ensure that existing legislative frameworks are clarified and fit for purpose. Our members report that the current landscape is extremely difficult for clients to navigate in terms of compliance and presents challenges for practitioners seeking to advise them.

QLS has previously submitted that at a minimum, a legal framework which appropriately reflects stakeholder interests in AI should consider:

- Liability risks: clarity as to who in the AI services supply chain carries legal risks of liability for breach of the law.

---

[20] Ibid, 486.

[21] Australian Government, 'National Strategy for Identity Resilience' *Department of Home Affairs* (Report, 23 June 2023) < https://www.homeaffairs.gov.au/criminal-justice/files/national-strategy-for-identity-resilience.pdf>

- Global consistency: the principles would be aligned with like best practice principles in ex-Australian laws, compliance with which is likely to be needed by Australian AI-related service providers doing business internationally.
- Human rights protection: it would require a baseline protection for individuals affected by the direct and indirect aspects of AI and ADM.
- Civil society transparency and accountability: it would require, where AI services may have adverse impacts on users or the individuals about whom the AI service is used, they are preceded by guaranteed and transparent safeguards.

The scope of AI technology development, use and risk is difficult to predict. QLS recommends that the Government should concurrently prioritise existing privacy, data and consumer related reform recommendations in this area and draw heavily on experiences from other like jurisdictions to progress a more harmonised approach globally.

Ethical responsibilities and AI software testing

There are three main actors in the use of AI:

- the manufacturers of the AI software;
- the data aggregators; and
- the end users (public and private sector entities) of the AI deployed.

Each of these parties have ethical responsibilities that must be considered.

Some of our members have also suggested there should be a gatekeeper approach before AI software is released. We understand that AI involves three sub technologies: a large data repository (which is the large language model), the inference engine (which is the analyser), and a set of sub technologies based on statistical analysis to create results and a feedback loop (which is the learning structure to advance the knowledge base of the AI engine). If the data is flawed at any stage of this process, greater errors will be produced in the results. The car industry provides a useful analogy and potential template for AI pre-release, that is, vehicles are not released to the public until there has been extensive design, testing and approvals.

To mitigate this, AI software should be subject to formalised testing and transparency requirements. Currently, with the exception of safety critical software deployed in aviation and automated vehicles, most AI software is not subject to testing in this way. A similar system could be utilised for AI. However, in order for this to be effective there needs to be a clear understanding as to what AI software comprises. Our committee members have emphasised that a highly specialist and independent entity would be required to devise and administer any testing regime.

Legal industry specific considerations

Lastly, QLS takes the opportunity to raise legal industry considerations in the context of considering industry specific responses to AI use.

Our members have queried whether there is a need for a specific framework or guidance on what can and cannot be completed by AI in legal practice, and the level of transparency required by legal practitioners as to the use of AI. Law practices are already using AI in various forms (including generative AI) and at varying levels. It is suggested that there should be consistency

across areas of practice and that any framework on AI use in legal practice should be clear and easily understood by consumers so as not to devalue legal services. Our members note the work currently being undertaken by the Centre for Legal Innovation in this area and the important role that law societies and institutes will play in providing guidance to their members.

We would be pleased to meet with representatives from the Law Council and other constituent bodies to discuss what steps, if any, ought to be taken to progress initiatives in this regard.

If you have any queries regarding the contents of this letter, please do not hesitate to contact our Legal Policy team via [redacted]

Yours faithfully

[redacted]

Chloé Kopilović
President

Attachment A

Other lessons from the timely example of Robodebt applicable to AI assisted decision-making include:

- **Assumption of error**: even with a human in the loop, the onus of proving the accuracy of an automated decision should not rest with the affected citizen. Despite the best of intentions users of AI systems will come to place over-reliance on ADM, treating system conclusions as findings of fact rather than just another piece of evidence. Where ADM has been used, all decisions should be reviewed de-novo, with the onus being on the decision maker to show that the conclusion is supportable through the application of explicable principles.

- **Transparency**: where any technology is deployed that involves any automated decision-making capability, the parties should be aware of this technology and how it may affect them at any time in the future. Where Artificial Neural Networks (**ANN**) have been used for ADM, the complexity of a decision-making process may be such that simply allowing inspection of the algorithms used is of little benefit to an affected party. For each decision made, the parties should be given easy access to the foundation data used, the assumptions applied to it (for example, in the Robodebt context, that income has been averaged) and the conclusions reached. Tools available from the development of Explainable AI (**XAI**) as a separate discipline are likely to be more useful in assisting appropriate review of decisions than attempts to adapt common law approaches of administrative review to unlock the AI black box.

- **Responsibility:** the chain of responsibility in decision-making using AI tools is complex and diffuse. It includes the software vendors, those who have selected the system and training data and those who employ it day-to-day. In this environment it may become unclear who bears ultimate responsibility for ensuring that the system is fair and accurate. Each system that makes important decisions affecting the rights of individuals should have a person or agency responsible for its output. Legal liability for harm may not invariably rest with this designated party. However, it is incumbent upon them to ensure alignment between their ethical commitments, their supervisory role, and the system's generated outcomes.

- **Continuous risk management by design:** the Robodebt data matching system altered over time, and at each stage important risk mitigation fell away. The risk management framework surrounding the use of an AI tool must adapt throughout the tool's life cycle. Simple risk analysis on design and implementation is not sufficient. A continuous process to test system accuracy and fairness is essential, and a risk management framework applied to significant alterations in process and use.