THE LAW SOCIETY
OF NEW SOUTH WALES

Our ref: BLC/PDC:BMsh12124

12 November 2024

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

By email: natalie.cooper@lawcouncil.au

Dear Dr Popple,

Treasury Discussion Paper – Review of AI and the Australian Consumer Law

The Law Society appreciates the opportunity to provide input for a Law Council submission in response to the Treasury Discussion Paper - *Review of AI and the Australian Consumer Law* (**Discussion Paper**). The Law Society's Business Law and Privacy and Data Law Committees contributed to this submission.

Our comments in response to the specific Discussion Paper questions are outlined below.

1. How well adapted is the ACL to managing the risks of consumer harm of AI-enabled goods and services now and into the future?

The Discussion Paper notes there are competing views regarding the adequacy of the Australian Consumer Law (**ACL**)[1] to protect consumers from unfair and unsafe business practices when buying artificial intelligence (**AI**)-enabled goods and services. We acknowledge the view that the legislation is principles-based and technology-neutral and therefore potentially capable of encompassing AI-enabled goods and services in a range of contexts. We also recognise that technology neutrality is an important guiding principle in developing regulatory frameworks with sufficient flexibility to adapt to rapid change without stifling innovation.

However, the capacity for AI to transform the consumer landscape is unprecedented and we consider that a recalibration of consumer protection laws to address emerging gaps and growing uncertainty is warranted. We have previously observed that the Government's proposed mandatory guardrails for AI in high-risk settings is limited in scope[2], as set out in our earlier submission (**attached**), and we agree with the Law Council that the gradual introduction of regulation across various sectors is appropriate.[3] Consideration of additional ACL safeguards should also be cognisant of existing and developing frameworks. Expanded

[1] Schedule 2 to the *Competition and Consumer Act 2010* (Cth).
[2] Law Society of NSW, *Mandatory guardrails for AI in high-risk settings*, 27 September 2024, 4, attached.
[3] Law Council of Australia, *Introducing mandatory guardrails for AI in high-risk settings: Proposals Paper*, 9 October 2024, 16, online: https://lawcouncil.au/publicassets/ec29ca86-8987-ef11-94a9-005056be13b5/4595Paper.pdf.

regulation of commercial practices that misuse personal or sensitive data collected by AI-integrated products may transect existing privacy and cybersecurity legislation. There are also a number of potentially overlapping legislation reviews and reform proposals including:

- The Australian Competition and Consumer Commission's (**ACCC**) Digital Platform Services Inquiry 2020-2025 Interim Report No.5 which recommends an economy-wide prohibition on unfair trading practices.[4] Notably, the Government has given in-principle support to this proposal.[5]
- The Consumer Guarantees and Supplier Indemnification review regarding proposed new penalties under the ACL.[6]
- The Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2024.[7]
- The Privacy and Other Legislation Amendment Bill 2024.[8]
- The Cybersecurity Legislation Package 2024.[9]

Our specific concerns in relation to gaps and uncertainties with respect to the application of the ACL to AI-enabled goods and services are set out in our responses below. We also provide suggestions for risk management measures to foster trust in the regulatory framework.

2. Does the ACL protect consumers of AI-enabled goods and services to the same extent as consumers of traditional goods and services covered by the ACL?

Despite the technology-neutral language of the ACL, there are distinctive features of AI-enabled goods and services that pose inherent challenges to determining where responsibility for a breach of consumer law should ultimately lie and the applicable enforcement mechanisms. Our members have identified the following characteristics as contributing to the difficulty in applying the ACL to AI systems, which results in less protection to consumers of these items than protections enjoyed by consumers of traditional goods and services:

Complexity of ownership and liability

The various components of digital goods, such as hardware and digital content, may be sold separately. AI-powered technologies may also be offered as intangible services alone. Whether an AI system is characterised as a product or service, numerous parties may be involved in its production and supply. Multi-layered and time-limited contractual and licensing arrangements create further complexity and risk. If the product or service fails, consumers may be required to interact with various parties in the supply chain including merchants, hardware manufacturers, software designers, and internet service providers. Engagement with a business, and the ability to exercise consumer guarantee rights, may be further frustrated where AI-enabled service chatbots have been deployed as the customer interface and connection with the appropriate representative cannot be made. These factors impede the tracing of the source of a defect or malfunction and the attribution of liability.

[4] ACCC, Digital Platform Services Inquiry 2020-2025 - Interim Report No.5 ("DPSI Interim Report No 5"), September 2022, 64, online: https://www.accc.gov.au/system/files/Digital20report.pdf.

[5] Treasury, Government Response to ACCC Digital Platform Services Inquiry, ("Government Response to DPSI") 8 December 2023, 1, online: https://treasury.gov.au/sites/default/files/2023-12/p2023-474029.pdf.

[6] Treasury, Consumer Guarantees and Supplier Indemnification under Consumer Law (Consultation) online: https://treasury.gov.au/consultation/c2024-583535.

[7] The Bill has been referred to the Environment and Communications Legislation Committee for inquiry and report by 25 November 2024, online: https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Environment_and_Communications/MisandDisinfobill.

[8] Introduced 12 September 2024 and currently before the House of Representatives, online: https://www.aph.gov.au/Parliamentary_Business/Bills_LEGislation/Bills_Search_Results/Result?bId=r7249.

[9] Parliamentary Joint Committee on Intelligence and Security, Cybersecurity Legislation Package 2024 (Inquiry) online: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/CyberSecurityPackage.

Interconnected and dynamic nature of AI systems

Because of the ability of AI systems to self-learn and develop, the concept of defect and fault must now be considered in an environment which extends beyond the point at which the product is placed on the market and is within the direct control of the manufacturer and supplier. We comment on how this challenge may be addressed in our response to question 6.

In addition, AI-enabled goods and services may be dependent on software upgrades for continued functionality, effectively tying the consumer to the provider in an ongoing relationship. A particular product may also rely upon add-on components that are exclusive to the provider. Unpredictability of performance following such upgrades makes it difficult to identify fault as it is unclear how far the concept of defect might extend along the supply chain following purchase by a consumer. The unexpected behaviour of some AI-enabled products also presents safety risks that are heightened for vulnerable consumers. We also comment further in our response to question 6 on the use of product safety standards to mitigate such harms.

3. Does the ACL impact the choices of suppliers and manufacturers of AI-enabled goods and services differently to other suppliers and manufacturers?

While the scope of the ACL to regulate AI-enabled goods and services remains uncertain, and given the data-driven nature of AI, some developers may seek to take advantage of new and evolving opportunities to manipulate data for commercial gain. We note that commercial conduct designed to influence consumer behaviour and exploit psychological biases, known as "choice architecture", can be harmful if it influences consumers to, "purchase unneeded or unsuitable products, spend more than they want to, receive poor-value items or service, choose an inferior seller or platform, or spend less time or effort searching for alternatives."[10] In a regulatory environment where there is doubt that AI-enabled goods and services are caught, and given the potential for AI to amplify these practices, it is easier to opportunistically "distort consumers' free and well-informed decision-making processes, for instance when presented with false impressions or deceptive interface designs (i.e., dark patterns)".[11] We comment further regarding a proposed prohibition on unfair trading practices to address dark patterns design practices, in response to question 6 below.

The ACL does not currently present an effective barrier to commercial practices such as the development and supply of manipulative AI which is potentially harmful to consumers. We note also the broader economic impact of unregulated manipulative AI which has been said to create, "market inefficiencies, requiring consumers to deploy resources they otherwise would not. The time and labour expended detecting and resisting AI-facilitated manipulation could be put to better use".[12]

4. Do the current or anticipated uses of AI-enabled goods and services present risks that reveal gaps in consumer protection under the ACL?

Yes. See our responses above.

[10] Gov.UK, Evidence review of Online Choice Architecture and consumer and competition harm, April 22, online: https://www.gov.uk/government/publications/online-choice-architecture-how-digital-design-can-harm-competition-and-consumers/evidence-review-of-online-choice-architecture-and-consumer-and-competition-harm.

[11] Christof Koolen, "Consumer Protection in the Age of Artificial Intelligence: Breaking Down the Silo Mentality Between Consumer, Competition, and Data" (2023) 2-3 *European Review of Private Law* 427-468, 448, online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4735380.

[12] Tegan Cohen, "Regulating Manipulative Artificial Intelligence" (2023) 20 *scripted* 203-242, 236, online: https://script-ed.org/wp-content/uploads/2023/02/Tegan-Cohen_February-2023.pdf?d=11072024.

5. **Is the application of the ACL to AI-enabled goods and services uncertain? If so, how and what impact does this uncertainty have on consumers, manufacturers and suppliers?**

Yes. See our response above.

6. **How might uncertainty in relation to AI-enabled goods and services be addressed within Australia's consumer protection framework?**

The Law Society suggests consideration of the following possible measures to address gaps and uncertainty in the application of the ACL to AI-enabled goods and product related services.

Mandatory product safety standard

As noted in the Discussion Paper, there are currently no mandatory AI-specific safety standards for consumer goods or services, and Treasury is assessing whether current safety standards (including the Voluntary AI Safety Standard[13]) effectively guarantee the safe and responsible use of AI-enabled goods and services. In our view, the consumer protection regime would benefit from the introduction of product safety standards for AI-enabled items including safety-by-design principles and clear instructions/warnings. The incorporation of AI into consumer products can affect safety by way of a software malfunction or other data input error that might cause a malfunction.

One area of growing risk where mandatory product safety standards may substantially mitigate consumer harm is the rise in exploitative use of technology against victim-survivors of domestic and family violence; for example, prescribing clear and simple settings explanations, product warnings and functionality to locally override remote activation.[14]

It is timely that the ACCC has announced emerging technology as one of its product safety priorities for 2024-2025.[15] The Law Society submits that the ACCC's findings should be considered during the Government's review of AI and the ACL.

Prohibition on unfair trading practices

As previously mentioned, the Government has given its in-principle support to a new economy-wide unfair trading practices prohibition and strengthening of the existing unfair contract term laws.[16] We endorse this proposal which, in our view, provides an important safety net to capture conduct that might otherwise fall outside of the prohibition on misleading and deceptive conduct under section 18 of the ACL. While we note the ACCC has enjoyed considerable success enforcing breaches of the prohibition by online businesses that have utilised obscure data collection and algorithmic practices,[17] it is widely acknowledged that the prohibition has been of limited use in ruling out unfair or manipulative practices such as the

[13] Department of Industry, Science and Resources, Voluntary AI Safety Standard | Department of Industry Science and Resources, 5 September 2024, online: https://www.industry.gov.au/publications/voluntary-ai-safety-standard.

[14] See Lesley Nuttall, "Five Technology Design Principles to Combat Domestic Abuse – IBM Policy Lab", IBM, 17 July 2020, online: https://www.ibm.com/blogs/ibm-anz/five-technology-design-principles-to-combat-domestic-abuse-ibm-policy-lab/; see also eSafety Commissioner, Tech-based domestic and family violence, 24 June 2024, online: https://www.esafety.gov.au/women/reduce-technology-facilitated-abuse.

[15] ACCC, Product Safety Priorities 2024-2025, online: https://www.accc.gov.au/about-us/accc-priorities/product-safety-priorities.

[16] Government Response to DPSI (n 5).

[17] See for example ACCC enforcement action reported in Media Releases, "Service Seeking to pay penalty for misleading online 'customer' reviews", 22 July 2020, online: https://www.accc.gov.au/media-release/service-seeking-to-pay-penalty-for-misleading-online-customer-reviews; and "Trivago to pay $44.7 million in penalties for misleading consumers over hotel room rates", 22 April 2022, online: https://www.accc.gov.au/media-release/trivago-to-pay-447-million-in-penalties-for-misleading-consumers-over-hotel-room-rates.

use of dark patterns.[18] AI-powered augmentation of dark patterns greatly increases the potential for undue influence of consumer decision-making and highlights the need for regulation.

Rebuttable presumption as to legal liability

The Law Society notes the Australian Human Rights Commission has recommended:

> **Recommendation 11** The Australian Government should introduce legislation that provides a rebuttable presumption that, where a corporation or other legal person is responsible for making a decision, that legal person is legally liable for the decision regardless of how it is made, including where the decision is automated or is made using artificial intelligence.[19]

Implementation of this proposal would facilitate the making of claims in liability cases where, as discussed under question 2 above, proving a defect and/or liability is more complex for AI-enabled goods and services. We agree that this measure would support transparency in decision making and incentivise appropriate evaluation of reliability and safety of AI systems, although we note that some stakeholders consider that legislation is unnecessary given existing legal frameworks governing liability including tort law and corporate disclosure rules.[20] On balance, we consider closer examination of the proposal is warranted, particularly in light of recent international developments with the adoption of analogous but broader presumptions and principles of causation.[21]

7. Are the remedies for a breach of the ACL appropriate for consumers of AI-enabled goods and services?

As mentioned in response to question 1 above, the Government is consulting on consumer guarantees and supplier indemnification to address existing challenges experienced by consumers and small businesses in obtaining remedies for consumer guarantee failures. Remedies in the ACL may not be fit for purpose for AI items comprised of components that may be characterised as both goods and services. Different remedies are available under consumer guarantees depending on whether the item supplied is a good or a service.[22] In addition, consumer guarantees may not apply to goods purchased for re-supply, or for use or transformation in manufacturing or production. It may be appropriate to consider definitional clarifications to accommodate these variables.

8. Are there barriers to consumers of AI-enabled goods and services accessing appropriate remedies under the ACL?

Yes. See our responses to questions 1, 2 and 7 above.

While we note the unfair contracts and consumer guarantee provisions of the ACL have extraterritorial application,[23] in practice it can be difficult to secure a repair, replacement or

[18] DPSI Interim Report No 5 (n 4) 67-9.

[19] Australian Human Rights Commission, *Human Rights and Technology* (Final Report, 2021) Recommendation 11, 194, online: https://humanrights.gov.au/our-work/technology-and-human-rights/projects/final-report-human-rights-and-technology.

[20] Ibid 79.

[21] Norton Rose Fullbright, Artificial intelligence and liability: Key takeaways from recent EU legislative initiatives, July 2024, online: https://www.nortonrosefulbright.com/en/knowledge/publications/7052eff6/artificial-intelligence-and-liability.

[22] In relation to supply of goods see s 261, ACL; in relation to supply of services see s 269, ACL.

[23] Section 5 (1) of the *Competition and Consumer Act 2001* (Cth) extends the application of the ACL to conduct outside of Australia by entities engaging in conduct outside of Australia when they carry on business in Australia.

refund from an overseas business.[24] We have already identified, in response to question 2, obstacles to engagement with suppliers of AI systems which may have complex ownership arrangements. We have also noted the use of AI tools by some organisations as the customer interface. Apart from the inherent unreliability of this evolving technology, including hallucinations and shutdowns, in our members' experience there is an increasingly limited ability for consumers to retrieve requisite evidence of their interaction with, and decisions made by, suppliers via these points of contact. We suggest that mechanisms to facilitate and trace consumer interactions with businesses trading in these items, including those located overseas, are examined in developing appropriate remedies for consumers.

9. Are the existing mechanisms contained in the ACL appropriate for distributing liability among manufacturers and suppliers of AI-enabled goods and services?

No, see our response to question 2 above.

10. What other issues not raised in this discussion paper relating to the application of the ACL to AI-enabled goods and services should be considered?

Generally, small businesses have fewer resources than larger developers to create customised plans for mitigating risks when applying AI technologies in the creation of goods or services for commercial supply. Small businesses may adopt generalised guidelines such as Standards Australia ISO/ IEC 4200:2023 – AI management systems and the Voluntary AI Safety Standard. In our view, consumers would benefit from further guidance targeted to small business developers to proactively encourage compliance with the ACL.

11. Are there international developments in consumer protection law and policy to which Australia should have particular regard when considering the application of the ACL to AI-enabled goods and services?

We suggest the following for consideration:

- United States Federal Trade Commission enforcement activity and, specifically, "Operation AI Comply" targeting the use/sale of AI technology in deceptive or unfair ways.[25]
- The European Union product liability regime including revisions to the *Product Liability Directive* and the introduction of the *AI Liability Directive* to ensure appropriate consumer protections for users of AI systems.[26]
- The *Colorado AI Act*, commencing 1 February 2026, which will impose new consumer rights and obligations on developers and deployers of AI systems including notification, correction and appeal rights. [27]

[24] We note the ACCC has acknowledged their limited capacity to assist, see ACCC, Consumer rights and guarantees, online: https://www.accc.gov.au/business/selling-products-and-services/consumer-rights-and-guarantees.

[25] US Federal Trade Commission, "FTC Announces Crackdown on Deceptive AI Claims and Schemes", Media release, 25 September 2024, online: https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-announces-crackdown-deceptive-ai-claims-schemes.

[26] See Norton Rose Fullbright (n 21). https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/739342/EPRS_BRI(2023)739342_EN.pdf.

[27] See Marian Waldmann and Marijn Storm, "Navigating New Frontiers: Colorado's Groundbreaking AI Consumer Protection Law Colorado", *Morrison Foerster*, 31 May 2024, online: https://www.mofo.com/resources/insights/240531-navigating-new-frontiers-colorado-s-groundbreaking-ai.

Please do not hesitate to contact Sonja Hewison, Policy Lawyer, on (02) 99260219 or sonja.hewison@lawsociety.com.au if you would like to discuss this in more detail.

Yours sincerely,

Brett McGrath
President

Encl.

THE LAW SOCIETY
OF NEW SOUTH WALES

Our ref: PDL:BMml270924

27 September 2024

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

By email: Nathan.MacDonald@lawcouncil.au; John.Farrell@lawcouncil.au

Dear Dr Popple,

Mandatory guardrails for AI in high-risk settings

Thank you for the opportunity to contribute to the Law Council's submission to the Department of Industry, Science and Resources in response to the Proposals Paper for introducing mandatory guardrails for AI in high-risk settings. The Law Society's Privacy and Data Law Committee contributed to this submission.

Defining high-risk AI

In our view, the principles-based approach to determining high-risk AI allows for flexibility and adaptability. This is consistent with our previous support for principles-based legislation that would allow for flexibility, adaptability and a futureproof framework for AI.[1]

However, from a compliance point of view, and to assist in the design of AI tools, we believe developers and deployers of AI would benefit from a list of practical examples under each of the proposed principles. Given the narrow scope of the Proposals Paper, focusing only on AI in high-risk settings, we believe there is benefit in being more prescriptive in giving examples of what constitutes high-risk. This is informed by the consideration that the risk appetite and the use of AI in decision-making across different industries can be substantially different, and the measure for 'adverse impact' may also differ.

Therefore, we believe more clarity and certainty will result in combining a principles approach with non-exhaustive lists of examples under each of the principles, similar to the guidance provided for the *Security of Critical Infrastructure Act 2018*.

In terms of whether Government should consider banning any high-risk use cases, we believe any regulatory response should carefully balance mitigating risk with enabling innovation in AI. In our view, there is merit in banning AI practices that have an unacceptable level of risk, that is, where the risk cannot be mitigated, or the consequences of the practice pose unacceptable and irremediable harm to individuals and communities. To balance this with not

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

stifling innovation in AI, any ban of AI practices could potentially be implemented by way of subordinate legislation, to allow sufficient flexibility while AI continues to evolve. We suggest any ban contain sufficient certainty in the definition and interpretation of the prohibited practice, and clarity about why the risk is unacceptable.

It may be instructive to refer to the AI practices that are prohibited under the European Union's Artificial Intelligence Act (EU AI Act), for their incompatibility with individual and collective rights and fundamental values, such as the rule of law.

AI practices prohibited under Article 5 of the EU AI Act include:[2]

(a) Subliminal techniques which can materially distort a person's behaviour by impairing their ability to make an informed decision in a way that causes, or is reasonably likely to cause, them significant harm.
(b) Exploiting the vulnerabilities of a person or specific groups of people (for example, due to their age, disability or economic situation) which can materially distort their behaviour in a way that causes, or is reasonably likely to cause, them significant harm.
(c) Social scoring systems based on known, inferred, or predicted personality characteristics which causes detrimental or unfavourable treatment that is disproportionate, or used in a context unrelated to the context in which the data was originally collected.
(d) Risk assessment systems which assess the risk of a person to commit a crime or re-offend (except in support of a human assessment based on verifiable facts).
(e) Indiscriminate or untargeted web-scraping for the purposes of creating or enhancing facial recognition databases.
(f) Emotion recognition systems in the workplace or educational institutions (except for medical or safety reasons).
(g) Biometric categorisation systems used to infer characteristics, such as race, political opinions or religion.
(h) Real-time, remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement except (subject to safeguards and within narrow exclusions) searching for victims of abduction, preservation of life, and finding suspects of certain criminal activities. Real time means live or near-live material, to avoid short recording delays circumventing the prohibition.

To our previous point about providing certainty to the definition of prohibited practices, we believe categories such as (e) and (f) might leave open for interpretation the meanings of 'indiscriminate' or 'untargeted', and 'emotional recognition'. If sufficient certainty is achieved, this could provide clear expectations and safeguards from the outset about the necessity of protecting fundamental rights and values, and remove ambiguity for organisations who might seek to interpret the principles in a way that compromises the rights of the end user.

Proposed mandatory guardrails

We acknowledge that 9 of the 10 proposed mandatory guardrails are identical to the Voluntary AI Safety Standard. We note the Voluntary AI Safety Standard has been mapped against Australia's AI Ethics Principles and broadly aligns with existing frameworks (such as the ISO 42001:2023 and the US National Institute of Standards and Technology's Artificial Intelligence Risk Management Framework). Our comments on each of the guardrails are below.

[2] Thomson Reuters UK, Practice Note: EU AI Act, https://uk.practicallaw.thomsonreuters.com/w-042-3394?transitionType=Default&contextData=(sc.Default)

Proposed mandatory guardrail	Law Society comments
1. Establish, implement and publish an accountability process including governance, internal capability and a strategy for regulatory compliance	We believe that the process for accountability needs to be a best practice process.
2. Establish and implement a risk management process to identify and mitigate risks	We believe specific examples of risk management processes or frameworks are necessary, particularly for an organisation that is the final end user of an AI system. We note the Proposals Paper suggests that risk should be assessed on a use case basis. However, this can be difficult for AI systems with multiple use cases, which supports our suggestion for examples of risk management processes to be provided.
3. Protect AI systems, and implement data governance measures to manage data quality and provenance	We believe developers and deployers would benefit from guidance that establishes the benchmark for data quality, data provenance, and data security.
4. Test AI models and systems to evaluate model performance and monitor the system once deployed	We suggest that the testing of AI models and AI systems on an ongoing basis needs to be performed by persons with accreditation in the subject matter. We also recommend for the testing to go beyond pure monitoring, such that the results are reported to an accountable authority within the organisation.
5. Enable human control or intervention in an AI system to achieve meaningful human oversight	We support this guardrail.
6. Inform end-users regarding AI-enabled decisions, interactions with AI and AI-generated content	We support this guardrail. Given the introduction of the Privacy and Other Legislation Amendment Bill 2024, we believe it would be beneficial for further clarity to be provided on the relationship between this guardrail and the Bill’s proposed requirement for disclosure in privacy policies if personal information is used in automated decision-making, which could involve AI systems.
7. Establish processes for people impacted by AI systems to challenge use or outcomes	We suggest the processes include clear guidelines for any challenge of the use or outcomes of AI systems to be dealt with in a timely manner, with clear communication mechanisms.
8. Be transparent with other organisations across the AI supply chain about data, models and systems to help them effectively address risks	We have consistently supported the need for transparency, on the basis that transparency brings robustness to AI regulation.
9. Keep and maintain records to allow third parties to assess compliance with guardrails	We suggest that the record-keeping processes should be consistent with external standards, with reference to

	examples such as the *Archives Act 1983* (Cth) or the *State Records Act 1998* (NSW).
10. Undertake conformity assessments to demonstrate and certify compliance with the guardrails	We understand that a 'conformity assessment' is intended to be an accountability and quality assurance mechanism that relies on documentation captured pursuant to Guardrail 1 and 9. We suggest that conformity assessments be carried out by an accredited third party, or by government entities or regulators, rather than the organisations themselves, and that the accountability and quality assurance metrics be standardised.

Regulatory options

As a general comment, we have long supported an interoperable AI regulatory framework, and advocated for consistency with related legislation, including privacy, data security, product safety, consumer protection, intellectual property, defamation, and human rights law.[3] We support the ability of consistent definitions across regulatory frameworks to facilitate greater certainty and compliance among industries.

We believe the principles-based approach to the guardrails would be assisted by enforcement through a legislative framework, which may allow for flexibility, while incentivising compliance through its legislative basis. An analogous model is the Australian Privacy Principles, which is given legal force by the *Privacy Act 1988*, but remains flexible, as the principles are interpreted by guidance.

In our view, option 2 appears to adopt a middle-ground approach between options 1 and 3. While option 1 appears to be beneficial for reducing the risk of inconsistency or duplication across regulatory frameworks, it is likely to be a more time-consuming project, given the need to review and amend existing laws to embed the guardrails.

The benefit of option 2 appears to be its ability to adapt existing regulatory frameworks and expand the powers of existing regulators to account for high-risk AI. However, given its reliance on amending existing laws, it is unlikely to capture AI developers, or other areas that existing laws do not apply to.

Option 3 might allow for Australia to be more consistent with the broader global scheme, given the recent implementation of the EU AI Act, and the UK's plan to introduce a standalone AI Act. This comment is also informed by the consideration that the guardrails are intended to only apply to AI in high-risk settings, thereby limiting the scope of application to a limited set of AI uses and outcomes. However, this approach will most likely result in overlap in existing laws and may require frequent amendment for currency to keep up with the fast-evolving pace of AI development.

[3] Law Society of New South Wales, Submission No 30 to the NSW Legislative Council, *Parliamentary Inquiry in Artificial Intelligence (AI) in New South Wales*, 20 October 2023, 7-9.

If you have any questions in relation to this submission, please contact Mimi Lee, Policy Lawyer, by phone (02) 9926 0174 or by email to mimi.lee@lawsociety.com.au.

Yours sincerely,

Brett McGrath
President