Law Council
OF AUSTRALIA

Safe and responsible AI in Australia

Department of Industry, Science and Resources

17 August 2023

Telephone +61 2 6246 3788
Email mail@lawcouncil.au
PO Box 5350, Braddon ACT 2612
Level 1, MODE3, 24 Lonsdale Street,
Braddon ACT 2612
Law Council of Australia Limited ABN 85 005 260 622
www.lawcouncil.au

Table of Contents

About the Law Council of Australia

The Law Council of Australia represents the legal profession at the national level, speaks on behalf of its Constituent Bodies on federal, national and international issues, and promotes the administration of justice, access to justice and general improvement of the law.

The Law Council advises governments, courts and federal agencies on ways in which the law and the justice system can be improved for the benefit of the community. The Law Council also represents the Australian legal profession overseas, and maintains close relationships with legal professional bodies throughout the world. The Law Council was established in 1933, and represents its Constituent Bodies: 16 Australian State and Territory law societies and bar associations, and Law Firms Australia. The Law Council's Constituent Bodies are:

- Australian Capital Territory Bar Association
- Law Society of the Australian Capital Territory
- New South Wales Bar Association
- Law Society of New South Wales
- Northern Territory Bar Association
- Law Society Northern Territory
- Bar Association of Queensland
- Queensland Law Society
- South Australian Bar Association
- Law Society of South Australia
- Tasmanian Bar
- Law Society of Tasmania
- The Victorian Bar Incorporated
- Law Institute of Victoria
- Western Australian Bar Association
- Law Society of Western Australia
- Law Firms Australia

Through this representation, the Law Council acts on behalf of more than 90,000 Australian lawyers.

The Law Council is governed by a Board of 23 Directors: one from each of the Constituent Bodies, and six elected Executive members. The Directors meet quarterly to set objectives, policy, and priorities for the Law Council. Between Directors' meetings, responsibility for the policies and governance of the Law Council is exercised by the Executive members, led by the President who normally serves a one-year term. The Board of Directors elects the Executive members.

The members of the Law Council Executive for 2023 are:

- Mr Luke Murphy, President
- Mr Greg McIntyre SC, President-elect
- Ms Juliana Warner, Treasurer
- Ms Elizabeth Carroll, Executive Member
- Ms Elizabeth Shearer, Executive Member
- Ms Tania Wolff, Executive Member

The Chief Executive Officer of the Law Council is Dr James Popple. The Secretariat serves the Law Council nationally and is based in Canberra.

The Law Council's website is www.lawcouncil.au.

Acknowledgements

The Law Council acknowledges the assistance of the following Constituent Bodies in preparing this submission:

- Law Society of New South Wales;
- Queensland Law Society;
- Law Society of South Australia; and
- Law Institute of Victoria.

The Law Council is also grateful for the contribution of its Futures Committee and the following Committees of its Business Law Section:

- Competition and Consumer Committee;
- Digital Commerce Committee;
- Intellectual Property Committee;
- Media and Communications Committee; and
- Privacy Law Committee.

Executive Summary

1. The Law Council welcomes the opportunity to provide a submission to the Department of Industry, Sciences and Resources (the **Department**) in response to the Discussion Paper on *Safe and Responsible AI in Australia* (**Discussion Paper**).[1]

2. Artificial intelligence (**AI**) has the potential to deliver significant opportunities and benefits across the economy and society more broadly, and can be expected to cause disruption and innovation in many key industries. The Law Council considers this to be a timely opportunity to consider reform in response to advancements in technology and the implications for the Australian public.

3. Existing AI governance mechanisms in Australia are largely voluntary and rely on general regulatory frameworks. In the Law Council's view, the significant risks posed by the use of AI justify a strengthened and precautionary approach to AI regulation, where there is evidence that existing laws and regulations are insufficient to address the issues and harms arising. Further regulation should be multifaceted. It should include the expansion of current legislation and, where necessary, new targeted legislation, not just a soft law approach of a voluntary code. However, the Law Council considers that the Australian Government should not seek to explicitly regulate AI via a comprehensive 'AI Act'.

4. The Law Council suggests the establishment of a dedicated interdepartmental taskforce to:

   (a) provide detailed, technical advice and guidance;

   (b) consider international developments;

   (c) provide a forum for collaboration / information sharing and consultation, and

   (d) coordinate consideration of AI regulation with state and federal agencies.

5. In the short term, the Australian Government should consider the regulation of high-risk AI technology and applications. In particular, enhanced regulation of the collection and use of biometric information (such as the use of automated facial recognition technology) and 'social scoring' practices, and options to reduce the risk of people being misled by AI-generated fakes and scams.

6. Further, following the release of the Final Report of the Royal Commission into the Robodebt Scheme,[2] comprehensive regulatory reform is required to ensure that the use of automated decision making (**ADM**), including by the Australian Government, is transparent, capable of review, and consistent with administrative law principles.

7. The Law Council does not, at this stage, advocate the adoption of any particular international regulatory model. 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.

[1] Department of Industry, Sciences and Resources (Cth), *Safe and Responsible AI in Australia* (Discussion Paper, June 2023) ('Discussion Paper').
[2] Final *Royal Commission into the Robodebt Scheme* (Final Report, July 2023).

Definitions

8. Given the inherently global nature of AI, the Law Council supports legislative and regulatory definitions of AI that are broadly consistent with existing approaches adopted in the United Kingdom (**UK**) and the European Union (**EU**).

9. Whilst there is no universally accepted definition of AI, the UK describes AI by reference to a combination of adaptivity and autonomy, being 'two characteristics that generate the need for a bespoke regulatory response'.[3] By comparison, the European Parliament recently proposed a refined definition of AI,[4] in alignment with the Organisation for Economic Cooperation and Development's *Principles for responsible stewardship of trustworthy AI* (**OECD Principles**)[5] and the United States National Institute of Standards and Technology's *Artificial Intelligence Risk Management Framework* (**NIST AI Risk Management Framework**).[6]

10. The amended definition included in the Draft Artificial Intelligence Act recently adopted by the European Parliament for negotiation with EU member states (**Draft EU AI Act**) refers to AI as 'a machine-based system that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate outputs such as predictions, recommendations, or decisions that influence physical or virtual environments'.[7]

11. Without alignment on the definition of AI, major trading partners may be deterred from engaging with Australian entities and consumers on significant economic and commercial activities.

12. The Law Council acknowledges that opportunities presented by certain AI models, including large language models (**LLMs**) and multimodal foundation models (**MFMs**), are almost impossible to forecast accurately over the next decade,[8] creating difficulty in crafting a suitably comprehensive definition. To mitigate this, any proposed definitions should be technologically neutral and sufficiently flexible to accommodate fast-paced technological developments.

13. The definitions could be enhanced with the inclusion of a definition relating to AI robotic systems. Deployment of autonomous AI, without real-time human supervision, such as in robot control, should be within the scope of any regulatory regime.

14. Moreover, any proposed definitions should be subject to regular review and be updated as necessary to reflect the changing understanding, knowledge, and application of AI systems.

---

[3] Department of Science, Innovation and Technology (UK), *A pro-innovation approach to AI regulation* (March 2023) 22.
[4] European Parliament, *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* (COM(2021)0206) as amended by 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* (P9_TA(2023)023) ('Draft EU AI Act').
[5] Organisation for Economic Cooperation and Development, *Recommendation of the Council on Artificial Intelligence* (OECD/LEGAL/0449) (Report, May 2019).
[6] National Institute of Standards and Technology, Department of Commerce (US), Artificial Intelligence Risk Management Framework (AI RMF 1.0) (January 2023).
[7] European Parliament, *Draft EU AI Act*, art 3(1) (as amended by Amendment 165).
[8] Discussion Paper, 9, citing Genevieve Bell, et al, Australian Council of Learned Academies, *Rapid Response Information Report: Generative Ai* (March 2023).

Governance and regulation

Current state of play

15. Innovation in AI technologies is at an early stage of development, and it is near impossible to ascertain how rapidly evolving AI technologies will impact upon the law and Australia's existing regulatory approaches.

16. Existing Australian AI governance mechanisms have been largely voluntary and rely on general regulatory frameworks embedded in consumer, competition, corporate, criminal, and privacy laws (among others).[9] Australia's Artificial Intelligence Ethics Framework (**AI Ethics Framework**) provides voluntary principles for designing and implementing AI responsibly.[10] The principles align with the OECD Principles and are intended to supplement existing regulations and practices.

17. Across international jurisdictions, a variety of alternative approaches have been explored, including, but not limited to, bans, the creation of standalone AI laws and specialist tribunals. However, single mechanisms such as these provide inadequate protection, and greater cohesiveness and further regulatory and governance responses will be required to mitigate emerging risks.

Approaching additional regulation

18. The Law Council supports both increased governance initiatives and—where there is evidence that existing laws and regulations are insufficient to address the issues and harms arising—enhanced regulatory measures to ensure that AI is developed, implemented, used, and made available safely in both the public and private sectors.

19. Any governance initiatives or enhanced regulation must balance the worthy objectives of encouraging Australia as a leader in developing and implementing AI applications to the benefit of Australians (recognising the dominance of foreign-owned and headquartered technology providers) while providing holistic protection from harm.

20. Any overarching regulatory framework should be principles-based, people-centric and underpinned by a range of supporting regulatory mechanisms.[11] Systems must be ethical, lawful, and technologically robust, rigorously reviewed and appropriately governed, incorporating appropriate risk allocation (taking into account relative bargaining power of the entities involved), to enable ongoing monitoring and reporting mechanisms, as well as avenues to contest decisions.

21. Whilst jurisdictions around the world have been cautious to avoid adopting 'a heavy-handed' approach to AI regulation which may potentially stifle innovation, 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 for ill-defined and rapidly evolving technologies, 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 often, lack the resources to challenge

[9] Discussion Paper, 10.
[10] Department of Industry, Sciences and Resources (Cth), *Australia's Artificial Intelligence Ethics Framework* (Web Page, 7 November 2019).
[11] World Intellectual Property Organisation, *WIPO Conversation on Intellectual Property (IP) and Artificial Intelligence (AI)* (Report, Third Session, November 2020) 4.

alleged AI abuses including ADM. In this regard, the Robodebt Scheme clearly emphasised the importance of transparency and AI-creator/user accountability to civil society in a context of increased adoption of ADM and the training and use of AI related technologies more broadly.[12]

22. There are laws that already apply to AI.[13] The growth of the digital economy, and changes to the way in which businesses engage with their supply chain and end users, is driving regulators in several specialist areas to consider the effectiveness of current regulatory frameworks. Building on Australia's existing regulatory regimes, further regulation of AI is required together with meaningful enforcement powers.

23. The development of safe and responsible AI in Australia requires an interoperable framework that will enable Australian organisations to innovate. It must also provide sufficient safeguards, including against infringement of others' pre-existing rights or assets, such as intellectual property rights, confidential information and personal information. The framework should be flexible, scalable, and future-proof. It is also critical that a harmonised approach is taken across regulation to ensure consistency, avoid duplication, and avoid fragmentation of regulation.

Flexibility

24. The framework should build upon, and be adapted to, existing processes that Australian organisations have in place—for example, enterprise risk frameworks and methodologies, software and other technology project assessment and management frameworks and methodologies, privacy and security by design and default, and privacy risk assessment. It must also be cognisant of existing laws, including as examples, privacy, data security, product safety, consumer protection, and human rights-based laws such as anti-discrimination statutes.

Scalable

25. Since data and provision of cloud-based services have no geographic boundaries, the framework must be scalable. As different regulatory models in diversely regulated jurisdictions apply at various points in a data-driven service supply chain, AI regulatory initiatives should be determined with reference to evolving regulation in other jurisdictions (see discussion beginning at paragraph 83 below). These models will impact both links in the AI supply chain and Australia's assessment of the extent of the impact and effectiveness of that regulation to achieve safe and responsible AI at the Australian end of that supply chain. The framework needs to take into consideration and leverage international initiatives that can facilitate responsible and accountable flows of data, and cross-border business models that enable Australian businesses to expand and compete globally and cost-effectively.

Future-proof

26. A future-proof framework will enable Australian organisations, as adopters of AI, as producers of AI and as detectors of AI-misappropriation.

27. The Law Council supports adaptability through the adoption of principles-based legislation, providing for legal responsibility and substantive accountability of entities across the AI service supply chain. This should include measures to ensure that entities have appropriate incentives to adopt risk of harms assessments, mitigation

[12] Final *Royal Commission into the Robodebt Scheme* (Final Report, July 2023) (Section 4: Automation and data matching).
[13] Discussion Paper, 10.

and management of residual risks, supported by a risk management framework. The risk management framework should broadly align to existing risk frameworks, as to some degree, the fundamental risks remain the same, only these risks are amplified together with the propensity for false information.

28. The Law Council supports technology neutrality as a key principle to underpin any new regulation of AI. Given the rate of change in technological development, the objective should be to avoid technology- or platform-specific laws that become redundant or only partially effective. Under such a regulatory framework, the question of *how* the analysis and/or decision is made or delivered is irrelevant, and it is the act of the analysis and/or decision made or delivered itself that is being regulated.

Developing further regulation

29. In approaching the development of further regulation, the Law Council supports adherence to the following principles:[14]

    (a) establishing a case for action before addressing a problem. The Discussion Paper references some possible harms to individuals arising from AI, but further consideration of AI technologies, AI applications and potential harms via a market study or other inquiry would help identify problems and design solutions that are targeted at those problems;

    (b) considering a range of feasible alternative policy options and assessing their benefits and costs;

    (c) adopting the policy options that generate the greatest net benefit for the community;

    (d) in accordance with the *Competition Principles Agreement*,[15] legislation should not restrict competition unless it can be demonstrated that:

        (i) the benefits of the restrictions to the community outweigh the costs; and

        (ii) the objectives of the regulation can only be achieved by restricting competition;

    (e) providing effective guidance to relevant regulators and regulated parties in order to ensure that the policy intent and expected compliance requirements of the regulation are clear;

    (f) ensuring that regulation remains relevant and effective over time;

[14] See further, Law Council of Australia, Submission to Digital Technology Taskforce, Department of the Prime Minister and Cabinet, *Positioning Australia as a leader in digital economy regulation – Automated decision making and AI regulation – Issues Paper* (3 June 2022) 7-8 <https://lawcouncil.au/resources/submissions/positioning-australia-as-a-leader-in-digital-economy-regulation---automated-decision-making-and-ai-regulation->. This list of principles is built on the 'Principles of best practice regulation' agreed by the Council of Australian Governments: Department of the Prime Minister and Cabinet, *Principles of best practice regulation* (2021). The Law Council notes that many of these principles are now reflected in the 'Principles for Australian Government policy makers' contained in: Department of Prime Minister and Cabinet, *Australian Government Guide to Policy Impact Analysis* (March 2023) 6.

[15] Council of Australian Government, *Competition Principles Agreement* (11 April 1995, as amended to 13 April 2007) 5(1).

(g) consulting effectively with affected key stakeholders at all stages of the regulatory cycle; and

(h) ensuring that any government action is effective and proportional to the issue being addressed.

30. While not addressed in the *Competition Principles Agreement*, the Law Council recommends that adherence to Australia's international human rights obligations—as these are interpreted in light of evolving AI challenges—is essential.[16]

31. Australia is a party to the seven key international human rights treaties and has also signed or ratified numerous optional protocols to those treaties. These international treaties, which Australia has voluntarily entered into, set out in clear terms Australia's international human rights obligations. Australia is bound to comply with their provisions and to implement them domestically. For that reason, regardless of the extent of any agreed overlap between the rule of law and human rights, it is entirely appropriate to evaluate government legislation, policy and practice by reference to its compliance with international human rights law.[17]

'Soft' law v 'Hard' law

32. AI technologies are rapidly evolving, and the applicable regulations and standards must be flexible to respond to developments in technology 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 help enable regulation to be sufficiently flexible to respond to changing technology and community expectations with respect to the development and use of AI.

33. The Discussion Paper notes that Australia's approach to date, in responding to emerging risks from AI, relies on a combination of:

- a broad set of general regulations that are mainly technology neutral (for example, consumer protection, online, safety, privacy and criminal);
- sector-specific regulation (for example, therapeutic goods, financial services, food safety and motor vehicle safety); and
- voluntary or self-regulation initiatives such as ethical principles for AI that provide guidance to businesses and governments for responsible design, development and implementation of AI (that is, a 'soft law' approach).[18]

34. Proponents of a soft law approach recognise 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 to new developments, limitations created by this flexibility include increased risk, greater uncertainty, reduced transparency and insufficient accountability.

---

[16] See United Nations Office of the High Commissioner for Human Rights, Artificial intelligence must be grounded in human rights, says High Commissioner (Statement, 12 July 2023) <https://www.ohchr.org/en/statements/2023/07/artificial-intelligence-must-be-grounded-human-rights-says-high-commissioner>.
[17] Law Council of Australia, Rule of Law Principles (Policy Statement, March 2011) <https://lawcouncil.au/publicassets/046c7bd7-e1d6-e611-80d2-005056be66b1/1103-Policy-Statement-Rule-of-Law-Principles.pdf> 2.
[18] Discussion Paper, 10-15.

35. While voluntary or self-regulatory measures may be appropriate for some issues, ultimately, the success of voluntary or self-regulatory measures depends on their uptake and the level of compliance. Voluntary or self-regulatory measures are unlikely to be appropriate for addressing conduct that has the potential to give rise to significant harm experienced by consumers and broader individuals, and where the incentives to address that harm are lacking.

36. However, introducing *ex ante* regulation in a sector that is fast moving, dynamic and innovative is particularly challenging because of the difficulty of confidently distinguishing between conduct that is harmful and conduct that is neutral or benefits consumers and other individuals, and the real risk that targeted rules could become quickly out-dated and stifle innovation.

37. General regulations have the benefit of being both flexible and capable of adaptation and application to a broad range of products/services and businesses. They can be a useful starting point for considering further regulation. It is important to note, when implementing general regulations, that these can be difficult for businesses to interpret and it is important that businesses receive sufficient guidance as to what that regulation means in practice.

A multifaceted approach

38. The Law Council supports a multifaceted approach to AI regulation built on enhancing current regulation where there is evidence that existing laws and regulations are insufficient to address the issues arising. Further regulation should be provided for within the expansion of current legislation, and where necessary, new targeted legislation, rather than solely through a soft law approach of a voluntary code. This allows for clarity to be provided for regulated businesses and will ensure that all AI businesses are treated in the same manner. However, a layered approach is appropriate, with the Government also releasing principles/guidelines for the private sector (that is, not limited only to the public sector) in the short term to provide support to businesses where organic deployment of AI is occurring.

39. If the Government identifies particular harms to individuals or businesses in Australia from AI technologies, or conduct by AI providers that is causing (or likely to cause) harms that are not adequately addressed by existing laws, it would be appropriate to consider introducing industry-specific regulation designed to address those harms. Regulators should be open to *sui generis* laws as there are likely to be occasions when technologies or industry break away from the current norms and a swift and bespoke response is required.

Product stewardship and transparency

40. The Law Council emphasises the importance of Australia's adherence to the OECD AI Principles, which include 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.

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.[19]

41. Product stewardship is an important component in any regulatory approach. Each party in the supply chain, from the original developer to the final supplier, must be accountable and responsible for the use of AI. This requires appropriate standards of transparency and disclosure at each stage in the supply chain. Transparency between organisations, as well as transparency or visibility to the regulator is essential. Organisations must understand how the AI product they deploy functions. Regulators must be able to verify there is appropriate risk management and that is functioning as intended. Without transparency, Responsible AI is not achievable.

42. The Law Council, therefore, supports a risk-based approach, with a strong focus on transparency, accountability and responsibility. This should be developed cognisant of global approaches to avoid unwanted difficulties or disconnects with the global economy.

Standalone 'AI Act' or expansion of current regulation

43. In considering the future responsible use of AI in Australia, a question arises as to whether Australia requires a standalone 'AI Act' or whether a preferable approach is to utilise existing regulatory frameworks and enhance their application to AI.

44. The Law Council considers the significant risks posed by AI use justify a strengthened and precautionary approach to AI regulation. However, at this time, the Australian Government should not explicitly regulate AI via a comprehensive 'AI Act'. Rather, it should adopt a multifaceted approach built on enhancing current regulation. It should encompass precautionary-principle and risk-based regulatory approaches, specific sector and use prohibitions (for unacceptable risks), and mandatory standards.

45. There is no international consensus on the appropriate regulatory model for AI. Given AI covers such a vast range of different issues, it is unlikely a suitable uniform approach will be formulated that Australia can or should leverage to design its own priority legislative reform.

46. An explicit AI Act will require significant revision in the short to medium term due to:

(a) technological changes in a range of different AI programs and systems (and potential exponential change):

(b) the ubiquity of embedded AI in products; and

(c) change in cultural norms around acceptable use of AI.

[19] Organisation for Economic Cooperation and Development, *Recommendation of the Council on Artificial Intelligence* (OECD/LEGAL/0449) (Report, May 2019) art 1.2.

Establishment of a dedicated AI taskforce

47. The Law Council recommends establishing a dedicated taskforce as soon as possible, which, at a minimum:

    (a) acts as an advisory body to provide detailed, technical advice and guidance on equivalent international approaches—and gaps and issues in our existing domestic frameworks;

    (b) reviews and observes global AI hard law (for example in the EU and China) and guideline-style soft AI law positions currently in force (for example, in Singapore and the United States) over a period of 18 months. This will allow Australia to learn from other jurisdictions and gauge how the different approaches work / do not work, as well as how they need to interact with global standards, prior to implementing our own reforms;

    (c) contextualises any need for explicit AI law within other Australian relevant regulatory and legal reforms (for example, reforms of digital assets, banking and payments, privacy, digital identity and data rights);

    (d) provides a forum for 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;

    (e) coordinates and works with relevant Federal and State agency stakeholders to:

        (i) review Federal and State laws to understand how the adoption of AI and autonomous algorithms will impact the application, interpretation and enforcement of those laws in the short, medium and long term; and

        (ii) understand what existing governance mechanisms and legal protections we already have that can mitigate the potential risks and harms of AI in a technologically-neutral way; and

    (f) (potentially) takes a more active role in representing Australia in international policy forums and standard-setting contexts.

48. At the conclusion of an initial 18-month period, the taskforce could make recommendations to Government for legislative reform, including how urgent those reforms are. It is important to note, however, that acting as soon as possible will allow the rules of the road to be set and avoid some problems arising. Action should be taken earlier, where there are identified existing problems and there is evidence that existing laws and regulations are insufficient to address these problems (see, for example, the section below on 'Regulation of high-risk technology and application').

Industry-specific regulation

49. The Law Council submits that industry-specific legislation should only follow where there is evidence that existing laws and regulations are insufficient to address the issues arising in identified sectors. The Law Council encourages the Government to undertake a thorough gap analysis to identify areas where existing laws (also taking into account existing reform processes) are inadequate.

50. The introduction of any industry-specific legislation should not be duplicative and unnecessary. While the Law Council accepts that industry-specific legislation or regulation may be appropriate in some circumstances, careful consideration should be given to any unintended consequences that may arise from having industry-specific legislation that overlaps with other regulation applying more broadly. Industry-specific regulation should apply across an industry or to a particular sub-set of an industry (for example, certain types of AI applications that are regarded as particularly high risk and have caused, or are likely to cause, serious harm), rather than apply only to specific 'large' or 'major' providers.

51. An approach that discriminates based on the size of a provider should only be pursued if there are clear and compelling reasons for doing so, including an informed assessment that the benefits of that approach outweigh the risks (including when compared to alternative options). The Law Council takes this view for the following reasons.

    (a) First, as the Discussion Paper observes, AI is a fast-paced technology (see, for example, the rise of ChatGPT). The speed of development and rate of growth of these AI applications means that targeting regulations at providers that are 'large' or 'significant' today may be insufficient to protect consumers and other individuals from harms caused by new or emerging AI applications that could be on a similar growth trajectory.[20]

    (b) Second, individuals (and Australian businesses) should be protected from harm regardless of whether they are dealing with a large or small provider of AI. The Law Council, in its submission on the Data61 CSIRO Discussion Paper *Artificial Intelligence: Australia's Ethics Framework*, expressed caution about linking levels of risk to numbers of persons affected.[21] The assessment of risk should recognise that an impact felt even only by one person could nevertheless have 'major' or 'critical' consequences, potentially including fundamental rights breaches experienced by that person. An insignificant or minor risk could only be said to arise if its consequences would also be minor.[22]

    (c) Third, imposing regulation that discriminates based on a provider's size would distort competition between AI providers and could have other unintended consequences, such as discouraging deployment of AI applications in Australia, reducing incentives to invest in Australia or encouraging uptake of AI applications that may be 'smaller' in size, but more prone to causing harm. The starting point for regulation should be regulation that creates a level playing field, unless there are credible and compelling reasons for departing from that.

    (d) Fourth, imposing regulation on large AI providers may overlook sources of greater harm. The Discussion Paper notes that many private and public organisations are already adopting voluntary measures. Smaller or emerging

[20] A regulatory framework could be designed in a way that enables swift expansion to capture such applications (for example via a designation mechanism). However, thought would need to be given to the appropriate designating body, designation criteria, how the designating body would obtain sufficient information about such applications to enable it to make an informed decision to designate and issues of procedural fairness (such as giving relevant applications the opportunity to be heard before being designated and sufficient time to prepare for compliance). This would also result in uncertainty about the application or potential application of the relevant regulations and could have implications for incentives to invest and innovate.

[21] Law Council of Australia, Submission to Department of Industry, Innovation and Science (Cth), *Artificial Intelligence: Australia's Ethics Framework* (28 June 2019).

[22] Ibid [122].

AI applications may not have the incentive, or resources, to develop and adopt similar voluntary measures. Without commenting on the content or effectiveness of the voluntary measures adopted by major firms, targeting regulation at firms which have implemented voluntary measures, rather than smaller or emerging AI providers that have not implemented any voluntary measures, would fail to address conduct that is more likely to cause harm to individuals and businesses in Australia.

(e) Finally, it may be challenging to determine a size threshold that is not arbitrary, and to assess whether an AI provider or application meets the threshold where relevant information may not be forthcoming.

52. New AI applications and uses will emerge. While. the Law Council agrees that targeted regulation based on the level of risk is an appropriate way forward, it may be difficult to assess the risk level of AI applications and uses that are newly emerging. Accordingly, any industry-specific regulation should be capable of applying to varying and evolving forms of AI uniformly and consistently.

Monitoring and review

53. Given the rapid development of AI, any framework, regulatory or otherwise, must be subject to shorter, accelerated review cycles than would ordinarily apply. The common statutory review period of five years will be insufficient. Use of AI is rapidly accelerating, and it is not yet clear all the tasks to which AI will be deployed. This makes it difficult to build adequate safeguards. As noted throughout this submission, a multi-faceted approach to regulation is therefore required to promote adaptability and effectiveness in responding to the opportunities and challenges of the continued development of AI. The recent high profile data breaches in Australia are examples of legislation—the *Privacy Act 1988* (Cth) (**Privacy Act**)—and established cybersecurity requirements, that are insufficient safeguards against bad actors. The exponential rate of change in this environment demands continuous monitoring.

54. A risk management approach where the operation of AI is subject to extensive monitoring and detection systems has merit. It aligns with cyber security principles adopted in the Australian Cyber Security Centre's *Information Security Manual* of 'Govern, Protect, Detect and Respond'[23] and also both the NIST AI Risk Management Framework of 'Govern, Map, Measure, Manage'[24] and the International Organisation for Standardisation (**ISO**)/International Electrotechnical Commission (**IEC**) risk management approach to AI.[25] Under these frameworks, the focus is on ensuring that adequate systems for monitoring and detecting issues are in place so that, when an adverse consequence does arise, it may be responded to quickly. This flexible approach rather than a more prescriptive and prohibitive approach can inform a governance framework that assesses risk and provides redress.

55. The Law Council considers many AI risks can be addressed by establishing appropriate 'detect and respond' incentives, so an upfront restriction or prohibition is not required or justified in most cases. It is also difficult to design appropriate and

[23] Australian Cyber Security Centre, Australian Signals Directorate, *Information Security Manual* (22 June 2023) 5.
[24] National Institute of Standards and Technology, Department of Commerce (US), Artificial Intelligence Risk Management Framework (AI RMF 1.0) (January 2023).
[25] International Organisation for Standardisation and International Electrotechnical Commission, *Information technology — Artificial intelligence — Guidance on risk management* (ISO/IEC 23894, 1st ed, February 2023).

upfront restrictions or prohibitions for AI applications, given the rapidly evolving, changing and unpredictably diverse ways in which AI is being used to assist humans.

56. Upfront restriction or prohibition may not be required or justified if:

- prompt detection of a significant harm to human or the environment is likely;
- financial recompense to affected persons is appropriate to redress their loss/damage;
- penalties are appropriately substantial; and
- recovery of damages or penalties is sufficiently likely that entities are incentivised to properly mitigate risks of relevant harms.

57. Each regulated entity should apply appropriate risk of harms assessment. Transparency requirements may ensure prompt detection of a significant harm to humans or the environment, and attribution of that harm to a particular AI activity conducted by a regulated entity, is sufficiently likely. Requirements as to transparency of the fact that an AI risk assessment has occurred, although not necessarily the content of the AI assessment, may also assist in creating incentives to ensure that risks have been appropriately mitigated by regulated entities.

Regulation of high-risk technology and application

58. There is no international consensus on the appropriate regulatory model for AI (see discussion below). A key question for consideration is therefore whether Australia requires any express statutory prohibition on high-risk AI systems or use cases that present unacceptable risk and which should be banned (as per the approach in the Draft EU AI Act).[26]

59. The Draft EU AI Act contemplates a category of AI that presents an unacceptable risk and should be banned. In that category are:

- practices that have a significant potential to manipulate persons through subliminal techniques;
- practices that exploit the vulnerabilities of specific vulnerable groups (for example, children and persons with disabilities); and
- AI-based social scoring done by public and private authorities.[27]

60. These listed practices are clearly egregious and pose significant risks to the privacy and way of life of Australians. Existing Australian legislation does not provide adequate protection in relation to all these practices.

61. At a minimum, a legal framework which appropriately reflects stakeholder interests in AI in the context of high-risk technology and application should consider:

- liability risks—who in the AI services supply chain carries legal risks of liability for breach of the law. In this context a mechanism analogous to a 'public

[26] European Parliament, *Draft EU AI Act*, art 5.
[27] Ibid.

officer' may be appropriate—in other words, a publisher of AI must identify a human being who is the nominated contact point;

- global consistency—the principles must be aligned with similar best practice principles in foreign laws, compliance with which is likely to be needed by Australian AI-related service providers doing business internationally;

- human rights protection—this would require protection for individuals affected by the direct and indirect aspects of AI and ADM in accordance with Australia's international human rights obligations; and

- civil society transparency and accountability—this would require, where AI services may have adverse impacts on users or the individuals about whom the AI service is used, that they are preceded by guaranteed and transparent safeguards. One mechanism to consider could be the levels of mandated disclosure in AI-generated content that it has been so generated.

Biometrics and the use of automated facial recognition technology

62. The collection and use of biometric information (such as that obtained in facial recognition technology) by both private and public sector organisations poses significant privacy implications.

63. Law enforcement agencies in Australia have reportedly embraced facial recognition technologies in recent years, at times in the absence of a suitable regulatory framework (or even organisational authorisation).[28] An example of this is the use of Clearview AI's social media-derived database by the Australian Federal Police, as well as police in New South Wales (**NSW**), Queensland and Victoria.[29]

64. The Identity-Matching Services Bill 2019 (Cth) was intended to provide the legislative underpinning for the use of facial recognition technology by Commonwealth authorities based on a Government database. However, the Parliamentary Joint Committee on Intelligence and Security in 2019 recommended it be redrafted to address the lack of attention to privacy and human rights safeguards [30] There were reports in 2020 that the database continued to be built regardless.[31] As of 2023, the website *idmatch.gov.au* states that relevant services are already available, and that the 'full range of services will become available to government

[28] See, eg, Monique Mann and Marcus Smith, 'Automated Facial Recognition Technology: Recent Developments and Approaches to Oversight' (2017) 40 *University of NSW Law Journal* 121, 122-123; Adam Fletcher, 'Government surveillance and facial recognition in Australia: a human rights analysis of recent Developments' (2023) 32(1) *Griffith Law Review* 30, 33-37.
[29] See, eg, Josh Taylor, 'Victoria Police distances itself from controversial facial recognition firm Clearview AI' *The Guardian* (online, 19 June 2020) <https://www.theguardian.com/australia-news/2020/jun/19/victoria-police-distances-itself-from-controversial-facial-recognition-firm-clearview-ai>; Office of the Australian Information Commissioner, *AFP ordered to strengthen privacy governance*, Media Release, 16 December 2021: <https://www.oaic.gov.au/updates/news-and-media/afp-ordered-to-strengthen-privacy-governance>; Justin Hendry, 'Facial recognition use "misunderstood": NSW Police', *InnovationAus*, 11 October 2022: https://www.innovationaus.com/facial-recognition-use-misunderstood-nsw-police>.
[30] Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Advisory report on the Identity-matching Services Bill 2019 and the Australian Passports Amendment (Identity-matching Services) Bill 2019* (October 2019) iii–iv.
[31] Sarah Basford Canales, 'You can't Ever Get Privacy Back': ACT Delays Uploading Driver Licences to National Biometric Database until Laws Pass Parliament' The Canberra Times (online, 11 October 2020) <https://www.canberratimes.com.au/story/6962043/you-cant-ever-get-privacy-back-act-delays-biometric-licence-upload>.

agencies over the next two years', despite the Identity Matching Services Bill having lapsed in 2022.[32]

65. The collection and use of biometric data forms part of the Government's current Review of the Privacy Act—specifically a proposal to impose a 'fair and reasonable' test on the relevant data handling practices.[33] Proposals to use biometrics for establishment and verification of identity (with consent) reiterate the need to prioritise and integrate AI and privacy and related reforms coherently, to ensure that existing legislative frameworks are clarified and fit for purpose.

66. The Human Technology Institute at the University of Technology Sydney, has noted that laws in Australia (and around the world) do not effectively regulate the use of facial recognition technology. It has proposed a model facial recognition law.[34] Given the potential for misidentification associated with algorithmic bias (as discussed at paragraphs 125–131 below), and consequences for individuals of being misidentified by law enforcement, the Law Council supports in principle a legislative framework being enacted to ensure lawfulness and compliance with human rights in this field.[35]

67. The Australian Human Rights Commission (**AHRC**) in its *Human Rights and Technology* Final Report (**2021 AHRC Report**) recommended a moratorium 'on the use of biometric technologies, including facial recognition, in high-risk areas of decision making.'[36] The Human Technology Institute notes that such moratoria have been put in place prohibiting the use of facial recognition technology in circumstances where human rights are most at risk in other jurisdictions.[37] Until a framework is put in place to ensure lawfulness and transparency, it would be prudent for a similar measure to be adopted in Australian as well.

Social scoring

68. The Law Council considers that the AI 'scoring' of citizens, where a social, ethical or moral matrix is applied through AI surveillance and acts as a form of 'currency' to promote deemed 'social good', is a fundamental violation of the right to privacy and reputation.[38]

69. Social scoring carries significant risk including by way of loss of autonomy, the potential for increased discrimination, and the potential for punishment without crime.

70. The Draft EU AI Act proposes prohibiting social scoring and real-time biometric identification in certain circumstances unless exceptions apply.[39] Consideration could be given to adopting a similar model in Australia. The Ethics Guidelines for Trustworthy AI produced by the Independent High-Level Expert Group on Artificial

[32] Australian Government, *ID Match* (Web Page) <https://www.idmatch.gov.au/>.
[33] Attorney-General's Department, *Privacy Act Review Report 2022* (16 February 2023) 116.
[34] Nicholas Davis, Lauren Perry and Edward Santow, *Facial Recognition Technology: Towards a Model Law* (Report, Human Technology Institute, September 2022) 5.
[35] Law Council of Australia, Submission to Parliamentary Joint Committee on Intelligence and Security (Parliament of Australia), *Review of the Identity-Matching Services Bill 2019 and the Australian Passports Amendment (Identity-matching Services) Bill 2019* (2 October 2019) 8-11.
[36] Australian Human Rights Commission, *Human Rights and Technology: Final Report* (Report, March 2021) 13.
[37] Nicholas Davis, Lauren Perry and Edward Santow, *Facial Recognition Technology: Towards a Model Law* (Report, Human Technology Institute, September 2022) 35.
[38] See, eg, *Victorian Charter of Human Right and Responsibilities Act 2006* (Vic), s 13.
[39] European Parliament, *Draft EU AI Act*, art 5.

Intelligence of the European Commission should also be strongly considered in this regard.[40]

71. The 'scoring' of individuals may be reasonable in certain circumstances where it is authorised under a regulatory framework which balances an individual's right to privacy against the protection of other public interests. For example, a person's 'credit score' is currently used to assist lenders to decide whether to give a person credit or lend them money. Credit scores are produced by credit-reporting bodies by entering certain personal information into statistical algorithms. The credit score indicates a person's 'creditworthiness', which is an assessment of a person's eligibility to get consumer credit, consumer credit history, and capacity to repay an amount of credit that relates to consumer credit. The use of this personal information in this way is regulated under Part IIIA of the Privacy Act, the *Privacy (Credit Reporting) Code 2014 (Version 2.2)* and the *Privacy Regulation 2013* (Cth).

Fakes and scams

Ensuring basic transparency in the use of AI technology to build trust and reduce the risk of people being misled by fakes and scams

72. In making contributions to this submission, members of the legal profession have identified the risks posed by AI-generated media including 'deep fakes' and other false material and uses in political and other contexts.

73. AI systems can produce light, sound, images, video, text and other phenomena (**AI artefacts**) which makes it very difficult if not impossible to distinguish AI artefacts from human artefacts. In some contexts, this will create a serious risk of humans relying on an AI artefact as if it was a human artefact, and acting to their detriment. In such contexts, there will be a strong incentive for deception and scamming using AI artefacts.

74. For example, an AI-generated sound or voice which is designed to mimic a sound or human voice that occurs without AI generation may mislead the hearer into thinking the sound or voice is genuine and cause them to act as if it were genuine to their detriment—perhaps a voicemail from a family member asking for money or keys.

75. Excellent quality AI 'fakes' have the potential (in some contexts, not all), to undermine human trust in AI technology and in a range of human interactions with AI technology as well as to facilitate scamming and deception. The implications for video evidence, for example, are also serious. Juries may be persuaded to harbour reasonable doubt about evidence that is in fact genuine. AI generated text is already causing issues of plagiarism and cheating in educational settings.

76. Scams and deception are age-old human practices and AI adds another means. But it is the high quality of the fakes that AI can produce, the difficulty of detection, and the potentially ubiquitous use of AI artefacts which exponentially increase the incidence of fakes and the risk of deception. This justifies consideration now of the need for transparency disclosures in the use of AI in some contexts, to reduce the risk of deception and loss of trust.

77. There are many existing civil and criminal laws that penalise deception and fraud. But these operate *ex post facto,* and assume the deception can be detected, and the perpetrator found and held to account by legal process. It is far from clear that AI fakes will be detected quickly, or that the person or system which created or used

[40] European Commission, *Ethics Guidelines for Trustworthy AI* (April 2019).

the fake will be discoverable. In addition, AI fakes may be used in broader propaganda and political causes rather than to cause economic harm to specific individuals.

78. To increase confidence in the use of AI systems and to enhance accountability and reduce the risk of deception by AI fakes will require a multi-faceted approach—a combination of regulation, technical means for detection and correction, education of the public and proactive takedown obligations.

79. The example of AI fakes is illustrative of the challenge in regulating AI. It is not the technology that is used to create a deep fake that is problematic, it is the purpose for which it was created, how it is used and how it is relied on. Australia's regulatory approach needs to ensure that the appropriate laws can be used to respond (for example, miscommunication/misinformation, fraud, defamation). As suggested in the Discussion Paper, technologies used by law enforcement to identify deep fakes may also be high risk.[41]

80. The Law Council urges the Government to consider creating a basic transparency obligation on the creators and users of AI systems. This is not intended as a full regulatory response to AI but as a minimum regulatory step at this stage even if the Government intends to take time to consider other regulatory steps. The basic transparency obligation would be:

    (a) to disclose that content has been created using AI and identify the AI system used where possible by a means that is included with the content and cannot readily be removed or disassociated from the content; and

    (b) in some contexts, to disclose the persons responsible for creating and disseminating the content.

81. There are significant details to be worked through as to the form and detail of the disclosure, to what extent it can be made irremovable from the content, and the contexts in which the disclosure is mandated. However, the Law Council considers that the Government should make a commitment to a basic transparency obligation for the reasons stated and consult on the details.

82. In this regard, the Draft EU AI Act contains a form of basic transparency obligation in Article 52. The Government might consider adapting Article 52 to the Australian context:

> ***Transparency obligations for certain AI systems***
>
> *1. Providers shall ensure that AI systems intended to interact with natural persons are designed and developed in such a way that natural persons are informed that they are interacting with an AI system, unless this is obvious from the circumstances and the context of use. This obligation shall not apply to AI systems authorised by law to detect, prevent, investigate and prosecute criminal offences, unless those systems are available for the public to report a criminal offence.*
>
> *2. Users of an emotion recognition system or a biometric categorisation system shall inform of the operation of the system the natural persons exposed thereto. This obligation shall not*

[41] Discussion Paper, 39.

apply to AI systems used for biometric categorisation, which are permitted by law to detect, prevent and investigate criminal offences.

3. *Users of an AI system that generates or manipulates image, audio or video content that appreciably resembles existing persons, objects, places or other entities or events and would falsely appear to a person to be authentic or truthful ('deep fake'), shall disclose that the content has been artificially generated or manipulated.*

   However, the first subparagraph shall not apply where the use is authorised by law to detect, prevent, investigate and prosecute criminal offences or it is necessary for the exercise of the right to freedom of expression and the right to freedom of the arts and sciences guaranteed in the Charter of Fundamental Rights of the EU, and subject to appropriate safeguards for the rights and freedoms of third parties.[42]

International coherence and consistency

83. The Law Council does not, at this stage, advocate for the adoption of any particular international regulatory model. However, there are significant benefits in the alignment of Australia's relevant legal principles and frameworks with those of other countries that Australians transact with, and whose legal systems largely reflects similar societal norms, where appropriate.

84. The development of a standalone new framework without adequate consideration of existing frameworks is not supported. If Australia were to adopt a bespoke approach that does not take into consideration global and international negotiations underway on AI, this disconnect may have a detrimental economic impact and limit our ability to harness the benefits of AI and adequately safeguard against the risks.

85. While international consensus has not yet been achieved on the appropriate regulatory model for AI, and a single uniform approach or framework may not emerge in at least the short term, there are lessons that Australia should learn (and continue to consider) from these emerging international approaches and proposals. Seeking to ensure that Australian approaches remain broadly interoperable with relevant overseas frameworks holds clear benefits for Australians and Australian businesses.

86. As AI is inherently multi-jurisdictional Australia would benefit from achieving a degree of coherence with international regulatory approaches. In particular, an interoperable approach would promote more consistent expectations of businesses and organisations operating in Australia, allowing them to grow in Australia and expand overseas, as well as promoting a similar baseline standard of protection for Australian individuals relative to individuals in other countries.

[42] European Parliament, *Draft EU AI Act*, art 52.

87. The regulation of AI is at an early stage globally. Different nations hold different views with respect to their preferred regulatory model: for example, a single, comprehensive framework covering AI generally (like the Draft EU AI Act), specific frameworks targeted at particular use cases or contexts (as in a number of US state and local jurisdictions), or a 'hub and spoke' approach that relies on implementation across the economy (as in the UK). However, common features are emerging that can serve as a guide for understanding and approaching the Australian context.

88. Some of the common features developing internationally include:

    (a) overarching principles, which articulate the values as well as the potential opportunities and risks that the framework seeks to take into account;

    (b) risk-based approaches, which effectively demonstrate the prioritisation of certain use cases or subject matter for regulatory attention (whether these are explicitly enumerated or evident from the focus of the framework at hand);

    (c) a recognition that existing law and legal frameworks will and should apply to AI even where a more comprehensive law is proposed (the Draft EU AI Act explicitly intersects with many other EU laws and instruments); and

    (d) reliance upon emerging technical frameworks and standards to provide clearer and more actionable guidance to businesses, organisations, government agencies and other stakeholders on how best to safely and responsibly implement AI, including under the Draft EU AI Act and as part of the NIST AI Risk Management Framework.

89. The Law Council suggests that these elements, many of which are mentioned in the Discussion Paper, can and should be adapted to any regulatory model implemented in Australia.

90. 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. However, if Australia monitors global developments for too long before participating in these policy initiatives and does not leverage its participation in existing international initiatives, it risks lagging behind, losing the benefits of shaping AI policy internationally and locally, and being exposed to these risks.

91. The Australian Government's approach of adopting a three-tiered system to classify AI tools as low, medium or high risk seems prudent and consistent with the international regulatory approach to date. In effect, evolving global AI regulatory frameworks suggest that the level of regulation should be proportionate to the perceived policy concern. The risk profile of particular AI tools may also guide the Government in considering the options and timeline for action.

92. In addition, it is clear that international forums and standard-setting bodies will be important contributors towards any emerging consensus in this area. The Law Council supports Australia's continued representation and active participation in these bodies for the purposes of ensuring that these developing norms and standards are fit for purpose for all Australians and Australian organisations.

93. Leveraging international frameworks, such as the one being developed by the International Organisation for Standardisation across more than 50 countries (including the EU, UK, and US), can assist in ensuring that Australia has a regime

that will enable it to consume AI products from international suppliers, as well as develop its own products for export.

Australia's place in the global economy

94. The Law Council supports the statement in the Discussion Paper that 'as a relatively small, open economy, international harmonisation of Australia's governance framework will be important as it ultimately affects Australia's ability to take advantage of AI-enabled systems supplied on a global scale and foster the growth of AI in Australia'.[43]

95. Australia's regulatory approach to AI should be consistent with Australia's unique economic conditions, and its place in the global economy. At present, Australian businesses and other organisations are net deployers and users of third-party AI services, rather than developers and suppliers of AI services. As noted above, there is value for Australian businesses in aligning the Australian approach, so far as is reasonably practicable and consistent with protection of Australian citizens, to the approaches followed in key regulating jurisdictions.

96. While it is appropriate to seek a degree of alignment with countries with whom Australia shares similar values (such as the UK and the EU), particularly in the short term, it is critical that the approach adopted does not entrench Australia as a net user of AI. Rather the approach adopted should provide for the longer term, by enabling Australian organisations to be developers and creators of AI, and so that it will be imbued with Australian values and ethics. If Australia remains a net user, this is likely to have adverse long-term economic and social repercussions.

Public sector uses of AI

97. Australia's regulatory framework should support organisations (whether public or private) and individuals as users or implementers of AI. One of the challenges in developing the responsible use of AI, specifically for Generative AI, is that access to many AI tools is unrestricted, and it is quite feasible that in any given organisation, unknown and unsanctioned uses of AI are already occurring. From a perspective of ensuring there are adequate systems for monitoring the use of AI in an organisation, there may be a role for an AI gatekeeper who is responsible for how and when AI is being deployed in the organisation.

98. Where an organisation uses AI developed outside Australia, subject to a different regulatory framework, and possibly imbued with a different value system, the organisation will need guidance to ensure the responsible use of AI. Whether the organisation is a government agency, private sector or a not-for-profit organisation, controls around the implementation of AI are needed through an appropriate risk assessment and management framework. That said, there are arguments to differentiate between private sector and public sector uses of AI and the associated governance obligations. For example, obligations to give reasons in the public sector must be supported by strong explainability and transparency practices.

[43] Discussion Paper, 26.

99. The Law Council does not support a broad distinction between the public and private sectors in the use of AI technologies. Due to the nature of AI and the current or possible future applications of AI, the rights of individuals may be significantly impacted by both public and private sector entities. To protect the rights of individuals sufficiently, both the public and private sectors must meet obligations for transparency, fairness and equity in their integration of AI technologies.

100. A harmonised approach for the regulation of AI technologies in the public and private sectors would promote greater understanding of the obligations and liabilities imposed upon organisations using AI systems. If the Australian Government is held to a different standard than the private sector, this may lead to confusion and inconsistency, particularly where the private sector may be carrying out functions on behalf of Government. A harmonised approach across the public and private sectors enables consistent education and consistent guidelines for all organisations.

101. However, the Law Council suggests that the Australian Government should act as a role model, leading by example, in the adoption of ethical AI and responsible technology practices. The Government should be a model user of AI, assisting the creation of appropriate behaviours and standards which can then be applied more broadly to the private sector's use of AI. The Australian Public Sector Values, Code of Ethics and Code of Conduct should apply to the integration of AI as a tool in the public sector.

102. On this basis, the Law Council recommends consideration of the NSW Government's Artificial Intelligence Assurance Framework. This framework was developed to assist NSW agencies design, build and use AI-enabled products and solutions, and to help agencies identify risks that may be associated with their projects. Consideration could be given to implementing a similar framework nationally.

103. The Australian Government should foster responsible AI practices in its own agencies by training staff to utilise AI ethically and to mitigate possible risks. The Law Council suggests that the Australian Government provide targeted education for staff on relevant AI topics, including AI integration, privacy impact assessments, and the limits of AI.

104. The Law Council also recommends the implementation of strong national strategies on AI with whole-of-government approaches to ensure consistency across agencies and implementation to reduce the risk of inconsistency between Commonwealth and state regulatory approaches.[44]

Concerns around 'automated decision making'

105. The application of AI systems to ADM processes requires consideration in the development of a regulatory framework to deal with AI. The Law Council acknowledges the stated focus of the paper is 'AI', however, there are important linkages. As noted in the Discussion Paper, 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.[45]

[44] See also Australian Human Rights Commission, *Human Rights and Technology: Final Report* (Report, March 2021) 105.
[45] Discussion Paper, 6.

106. In relation to public sector use of AI and ADM, increasingly, new and amended Commonwealth Acts are empowering senior Commonwealth officials to arrange for the use of computer programs to exercise statutory powers and functions, including to make, and assist in making, administrative decisions—instead of human officials.

107. In May 2022, the Law Council of Australia made a comprehensive submission in relation to the *Positioning Australia as a leader in digital economy regulation—Automated decision making and AI regulation* Issues Paper, published by the Digital Technology Taskforce in the Department of Prime Minister and Cabinet (**2022 LCA Submission**).[46] This submission considered, in detail, public sector use of ADM.

108. The Law Council considered that there are evident public benefits in the increased deployment of AI and ADM, where this is done appropriately and judiciously. Those benefits can include increased efficiency, consistency, and accountability in decision making by government agencies. However, the Law Council considered that the threshold objective of regulation in relation to public sector use of AI and ADM is to ensure that it is employed consistently with administrative law principles which underpin lawful decision making—lawfulness, fairness, rationality, and transparency.

109. The Law Council considered that comprehensive regulatory reform is required to ensure that Commonwealth legislation which authorises the use of ADM and AI to exercise statutory powers is consistent with administrative law principles. Specifically, the Law Council recommended that:

    (a) the Australian Government commission an audit of all current or proposed use of AI and automation to make or assist in making administrative decisions by or on behalf of Government agencies;

    (b) legislative amendments be made to ensure that where it is intended that a statutory power be exercised by using ADM or AI, the statute expressly authorises the use of ADM or AI;

    (c) all legislation which authorises the use of ADM and AI to exercise, or assist in the exercise, of statutory powers should:

        (i) be consistent with regard to types of powers which may be exercised by ADM or AI, and employ standard statutory language for expressing the power to use ADM or AI;

        (ii) require an assessment be undertaken of the suitability of the proposed automated system to exercise the statutory power, as a precondition to making arrangements for use of AI or ADM;

        (iii) require that all arrangements for the use of ADM be subject to ongoing governance requirements by a multidisciplinary team to ensure they remain lawful and up to date, including auditing, testing and reporting obligations;

        (iv) require that officials publish all arrangements for the use of ADM and any suitability assessment which underpins it, including sufficient

[46] Law Council of Australia, Submission to Digital Technology Taskforce, Department of the Prime Minister and Cabinet, *Positioning Australia as a leader in digital economy regulation – Automated decision making and AI regulation – Issues Paper* (3 June 2022) <https://lawcouncil.au/resources/submissions/positioning-australia-as-a-leader-in-digital-economy-regulation---automated-decision-making-and-ai-regulation->.

information to enable a broad understanding of how AI or ADM operates to produce lawful administrative decisions;

(v) require that any affected individual must be notified where there is significant use of automation, including AI, in making an administrative decision;

(vi) require that an automated decision must be capable of being reduced to a statement of reasons explicable by a human, produced by a full audit trail of the decision-making path, for the purpose of enabling it to be reviewed by a tribunal or court, and the person affected by the decision should have a right to request such reasons; and

(vii) provide for the automated decision to be subject to review, preferably review by a human internal to the agency, and the person affected by the decision must be informed of that review avenue.

110. The Law Council considers that these principles remain relevant to the current consultation and refers the Department to the 2022 LCA submission.[47]

111. Currently, there is a lack of guidance as to the contexts in which ADM should be permitted for use—and there is an additional concern that ADM processes currently operate largely without transparency.

112. Transparency is critical for the responsible use of ADM by Australian organisations, both in the public sector and private sector. Individuals should know when and how ADM is being used in any way which significantly affects their human rights, their legitimate expectations to be informed of how and why they are being singled out for differentiated treatment, and their legitimate expectation that an automated decision is reasonable having regard to the circumstances in which it is made and the impact that this automated decision might reasonably be expected to have on affected humans and the environment.

113. The Law Council notes concerns about the 'black box' nature of some advanced AI using machine learning to make decisions, where the reasoning behind decisions cannot be traced or adequately explained. Regulatory responses should specifically articulate an obligation for manufacturers and organisations to avoid ADM algorithms that lack the ability to assess or test their decision-making (including any bias in its decision-making). In the Report of the Royal Commission into the Robodebt Scheme, Commissioner Holmes AC SC said, about system design, that:

> *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'.*[48]

[47] Law Council of Australia, Submission to Digital Technology Taskforce, Department of the Prime Minister and Cabinet, *Positioning Australia as a leader in digital economy regulation – Automated decision making and AI regulation – Issues Paper* (3 June 2022) <https://lawcouncil.au/resources/submissions/positioning-australia-as-a-leader-in-digital-economy-regulation---automated-decision-making-and-ai-regulation->.
[48] *Royal Commission into the Robodebt Scheme* (Final Report, July 2023) 486.

114. This is consistent with Recommendation 6 of the 2021 AHRC Report that states:

> *The Australian Government should make clear that, where a person has a legal entitlement to reasons for a decision, this entitlement exists regardless of how the decision is made. To this end, relevant legislation including s 25D of the Acts Interpretation Act 1901 (Cth) should be amended to provide that:*
>
> *(a) for the avoidance of doubt, the term 'decision' includes decisions made using automation and other forms of artificial intelligence*
>
> *(b) where a person has a right to reasons the person is entitled also to a technical explanation of the decision, in a form that could be assessed and validated by a person with relevant technical expertise*
>
> *(c) the decision maker must provide this technical explanation to the person within a reasonable time following any valid request.*[49]

115. Where decisions affecting individuals are permitted to be made through ADM processes, the Law Council submits that proper scrutiny by humans must be applied to ensure conclusions reached amount to 'decisions' for the purposes of the relevant legislation, and to encourage public confidence in Government agencies and their decisions. The circumstances surrounding the Robodebt Scheme, and the decision in *Pintarich v Deputy Commissioner of Taxation* (2018) 262 FCR 41, identify a need for better regulation and oversight of automated decisions.

116. People affected by fully or partially automated decisions by Australian Government agencies should not be precluded from accessing administrative law review and accountability mechanisms, such as the Commonwealth Ombudsman, merits review and freedom of information applications. Access to these forms of review was restricted throughout the operation of the Robodebt Scheme. The impact of restricting access to administrative law forums is evident in the erosion of public trust that resulted from that program. The costs associated with implementing accountability will ultimately result in better systems and processes with more obvious integrity.

117. ADM processes should be subject to regular random audits conducted by a human, to ensure any errors or potential for bias are identified. Further, any ADM and AI processes that directly affect individual rights and freedoms should have some level of human oversight, and the ability for humans to intervene and the opportunity for review by a human.

118. In this respect, the Law Council supports the establishment of an oversight body as proposed in Recommendation 17.2 of the Royal Commission Report. The Royal Commissioner recommended the Government 'should consider establishing a central regulator, or expanding an existing body, with the power to monitor and audit automated decision-making processes with regard to their technical aspects and their impact in respect of fairness, the avoidance of bias, and client usability'.[50] Such a role could be part of an overarching body with responsibility for the supervision of AI more broadly, including ADM. A new regulatory body of this nature would require sufficient resourcing to be effective.

---

[49] Australian Human Rights Commission, *Human Rights and Technology* (Final Report, 1 March 2021) 62 (recommendation 6).
[50] *Royal Commission into the Robodebt Scheme* (Final Report, July 2023) 488 (recommendation 17.2).

119. In addition to transparency, there is a current lack of guidance as to the contexts in which ADM is appropriate. In Australia, the principles governing automated systems are the Australian AI Ethics Principles (**AI Ethics Principles**) which form part of Australia's AI Ethics Framework.[51] The AI Ethics Principles were published in 2019 and dictate the ways in which AI systems (encompassing ADM) should operate to meet ethical standards, on a macro level only.[52] The Law Council suggests the OECD Principles could be used as a model for a principles-based and technologically-neutral overarching guideline for AI and ADM processes in Australia.[53]

The importance of data

120. Design of any AI governance framework must recognise:

    (a) the critical significance of data for the training, validation and testing of new AI systems and for updating and maintaining existing AI systems; and

    (b) the vital importance that will need to be placed on control of, and access to, data by any AI governance framework.

121. Data is—and will become increasingly—a strategic and highly valuable resource. This will require strong protections and foundational legal frameworks to protect public and personal data rights.

122. Ongoing law reform processes in respect of Digital Platforms and the Privacy Act are seeking to address the strategic importance of data in the digital economy. This is highly relevant to AI and therefore, consideration of AI in this context needs to be harmonised with other reform processes and Australia's legal frameworks. All reforms relating to data, should be interoperable and consistent to provide an appropriate framework for protection.

123. The Law Council suggests that the *Competition and Consumer Act 2010* (Cth) should be reviewed to identify necessary reforms to protect against data monopolies and new monopolistic actions that are harmful to consumer rights but would not be captured under existing concepts of aggregations or misuse of market power. The ACCC currently has a mandate to review digital platform services effectively by looking at data in vertical sectors. The Law Council suggests that the ACCC be tasked to identify the best way to capture and protect the value of data (considering risks of aggregation and use of data) horizontally across the economy rather than solely in vertical sectors.

124. Further, Australian privacy law reform should consider how regulation of certain categories of data and the use of data could provide effective governance of, and protections in relation to, AI systems rather than seeking to regulate AI technology which risks deterring innovation.

[51] Department of Industry, Sciences and Resources (Cth), *Australia's Artificial Intelligence Ethics Framework* (Web Page, 7 November 2019).
[52] *Royal Commission into the Robodebt Scheme* (Final Report, July 2023) 479.
[53] Organisation for Economic Cooperation and Development, *Recommendation of the Council on Artificial Intelligence* (OECD/LEGAL/0449) (Report, May 2019).

Human rights and AI

Algorithmic bias

125. The Discussion Paper identifies that '[a]lgorithmic bias is often raised as one of the biggest risks or dangers of AI' and further notes the major focus on this issue in the 2021 AHRC Report.[54] Bagaric, Hunter and Stobbs provide an overview of the use of algorithms in data-driven AI:

> *In crude terms, current data-driven artificial intelligence systems synthesize large amounts of data involving prior action or behavior to make predictions about future behavior. The way in which the data is processed is the key to the efficacy and integrity of AI. The data is processed by a formula, termed an algorithm.*
>
> *…*
>
> *Artificial intelligence uses algorithms to process and synthesize vast amounts of information and provide answers to problems. Thus, there is an inextricable connection between algorithms and artificial intelligence. All artificial intelligence systems are based on algorithms, however, most algorithms do not operate within the context of an artificial intelligence construct.*[55]

126. Data-driven AI enables intentionally or unintentionally differentiated treatment of individuals and groups in Australian society. This differentiation may result in bias or other errors. Data-driven AI outputs may be based upon, create or amplify misinformation or disinformation, or produce results that are otherwise unreliable or unsafe for the reliance that humans place upon them. Data used to produce those outputs may reveal information about an individual person's characteristics, interests, attributes and activities in both public and private spaces.[56]

127. Both regulated personal information, and other non-identifying information, may be used in ways that are beneficial, or in ways that are unreliable, unsafe or otherwise cause harms to those whose data has been used, impacting their human rights[57] and legitimate expectations to be informed of that use. The question of when uses of AI are reasonable, appropriately transparent and justified, is broader than legal assurance of protection of the right to privacy and other human rights. That noted, it is crucial that the human rights impact, including the privacy impact of the operation of AI should be part of the key considerations in determining Australia's framework.

128. Algorithmic bias, particularly its potential impact on vulnerable people, should be addressed through appropriate risk management processes. The responsible use of AI must address questions of fairness dictated by the required context. It must include safeguards to manage both data quality and human bias. Such safeguards

---

[54] Discussion Paper, 8.
[55] Mirko Bagaric, Dan Hunter, and Nigel Stobbs, 'Erasing the Bias Against Using Artificial Intelligence to Predict Future Criminality: Algorithms are Color Blind and Never Tire', (2020) 88 *University of Cincinnati Law Review* 1037, 1041-42.
[56] See eg Australian Human Rights Commission, *Using artificial intelligence to make decisions: Addressing the problem of algorithmic bias* (Technical Paper, 2020) 16-17.
[57] Most particularly, the right to privacy and home life in Article 17 of the *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976).

should be designed with Australia's international human rights obligations—and relevant research[58]—in mind.

129. The 2022 LCA Submission discussed, by way of example, the critical need for transparency in the use of AI and algorithm-informed automated-decision making in immigration detention.[59] That submission also addressed the appropriateness of deploying automated systems which use data-driven machine learning to exercise a statutory discretion in administrative decision-making.[60] Relevantly to the present discussion, the Hon Justice Perry of the Federal Court of Australia notes that machine learning is also subject to bias (footnotes removed):

> *While it may seem odd to speak of bias in the context of machines, "[p]rogrammers can build matching algorithms that have biased assumptions or limitations embedded in them. They can unconsciously phrase a question in a biased manner." Furthermore, biases may become embedded and reinforced through the process of machine learning.*[61]

130. When Australian consumers use AI, they may be exposed to AI which has been developed by technical experts with limited or no training in ethics or human rights, and without appropriate oversight. The challenge for consumers is that they do not have visibility of any incorrect decisions made about them using AI and data.[62] Without further detail, merely notifying consumers that an AI system is being used is likely to provide insufficient redress when a consumer is adversely impacted. Similar issues arise in respect of the limitation of privacy notices in providing adequate consumer protection. Careful consideration of appropriate remedies is required. Liability should be considered in light of existing product laws and developments, such as the EU Artificial Intelligence Liability Directive.[63]

131. Closely aligned with an approach based on human rights is a harm-minimisation approach, which considers the potential harms to humans and regulates accordingly. The approach adopted in Canada is anchored to its human rights regime but is articulated in terms of reducing the risks and harms associated with AI.[64] Until a federal human rights Charter is adopted in Australia (as the Law Council recommends),[65] it may be appropriate to frame these considerations through the lens of harm minimisation.[66]

---

[58] See, eg, Australian Human Rights Commission, *Using artificial intelligence to make decisions: Addressing the problem of algorithmic bias* (Technical Paper, 2020); Office of the Victorian Information Commissioner, *Artificial Intelligence and Privacy – Issues and Challenges* (August 2018).
[59] Law Council of Australia, Submission to Digital Technology Taskforce, Department of the Prime Minister and Cabinet, *Positioning Australia as a leader in digital economy regulation – Automated decision making and AI regulation – Issues Paper* (3 June 2022) [143]-[156].
[60] Ibid [99]-[109].
[61] The Hon Justice Melissa Perry, *iDecide: Digital Pathways to Decision* (Speech, Law Council of Australia 2019 CPD Immigration Law Conference, 21 – 23 March 2019) 8.
[62] Saurabh Bagchi, 'What is a black box? A computer scientist explains what it means when the inner workings of Ais are hidden', *The Conversation* (online, 22 May 2023).
[63] See International Organisation for Standardisation and International Electrotechnical Commission, *Information technology — Artificial intelligence — Treatment of unwanted bias in classification and regression machine learning tasks* (ISO/IEC CD TS 12791 C 23894).
[64] Discussion Paper, 20-21.
[65] Law Council, *Federal Human Rights Charter Policy* (November 2020) <https://lawcouncil.au/resources/policies-and-guidelines/federal-human-rights-charter>.
[66] European Parliamentary Research Service, *Artificial intelligence liability directive* (Briefing – EU Legislation in Progress, February 2023).

Competition and consumer issues

Consumer law issues

132. The Discussion Paper acknowledges that the potential risks of AI are currently governed by both general regulations and sector-specific regulations, including the *Australian Consumer Law* (**ACL**)[67] and competition law.

133. There are currently general and specific provisions in the ACL which seek to provide mechanisms to protect businesses and consumers, and which would appear to be capable of applying in various AI contexts. This includes:

    (a) Section 18 of the ACL which prohibits businesses from engaging in misleading or deceptive conduct in trade or commerce. Additionally, sections 29 and 33–36 prohibit businesses from engaging in various forms of false, misleading, or deceptive conduct in connection with the supply of goods or services. As noted in the Discussion Paper, the prohibitions on misleading conduct have been successfully used to pursue misleading algorithmic decision making.[68]

    (b) Sections 20 and 21 of the ACL which prohibit businesses from engaging in unconscionable conduct when dealing with other businesses or their customers. Unconscionable conduct means conduct that is so harsh it goes against good conscience.

    (c) Section 23 of the ACL provides that a term of a standard form consumer contract or small business contract that is unfair is void. Recent amendments to the unfair contract terms regime will make the use of unfair contract terms illegal and introduce significant penalties for breach of these provisions, from 9 November 2023. These provisions could apply to terms and conditions on which AI applications are offered to consumers or small businesses (noting the broader definition of small business that will apply from 9 November 2023), preventing terms that are unfair (such as limitations on liability or exclusion of liability for losses caused or contributed by the provider's negligence or recklessness, or opaque requirements to consent to data use/disclosure that may cause detriment to the user).

    (d) Sections 51–63 of the ACL contains consumer guarantees that apply to the supply of goods and services. These provisions would apply to AI applications to the extent they are goods or services supplied to a consumer in Australia. Relevantly:

        (i) the definition of 'goods' in subsection 2(1) includes 'computer software';[69]

        (ii) the definition of 'services' in subsection 2(1) includes any 'benefits…that are, or are to be, provided, granted or conferred in trade or commerce';

        (iii) under section 3, a person is a consumer if they have acquired goods for less than $100,000 (or a greater amount prescribed) or the goods were

[67] *Competition and Consumer Act 2010* (Cth) sch 2 ('*Australian Consumer Law*').
[68] See, eg, *Australian Competition and Consumer Commission v Trivago N.V.* [2020] FCA 16 (20 January 2020).
[69] The application of the ACL to downloadable computer software was considered in *Australian Competition and Consumer Commission v Valve Corporation (No 3)* [2016] FCA 196.

of a kind ordinarily acquired for personal, domestic or household use or consumption;

(iv) the consumer guarantees relating to acceptable quality, fitness for purpose, supply of goods by description and due care and skill would appear capable of applying to at least some AI applications; and

(v) as noted in the Discussion Paper, the ACL contains various remedies for breach of the consumer guarantees.

(e) Provisions of Part 3-3 of the ACL (relating to safety of consumer goods and product related services) would also appear to be capable of applying to some AI applications. 'Consumer goods' are goods either intended to be used, or of a kind likely to be used, for personal, domestic or household use or consumption (see subsection 2(1) of the ACL).

(f) Part 3-4 of the ACL (relating to information standards) would also appear to be capable of applying to some AI applications. This part is not limited to consumer goods or services supplied to consumers. Section 134 empowers the Commonwealth Minister to make information standards which can require the provision of specified information. The Part outlines the consequences of not adhering to such standards.

(g) Part 3-5 of the ACL (relating to liability of manufacturers for goods with safety defects) could also be applicable in some circumstances—for example, if the AI application in question is a 'good' and it has a 'safety defect' that causes injury to an individual. 'Manufacturer' has a broad meaning under section 7 of the ACL, which would appear to be capable of applying to suppliers and developers of AI applications. Goods have a safety defect if their safety is not such as persons generally are entitled to expect (section 9 of the ACL). However, it is not a requirement that goods are entirely free from risk.

134. The Law Council considers the Australian Government should consider whether existing competition and consumer laws may be adequate to deal with any conduct of concern or harms arising from AI applications. It is difficult to do this in the abstract.

135. While the Discussion Paper outlines some potential challenges for or concerns from AI, there is a lack of detail about AI technologies and applications that are currently in use in Australia and the specific concerns or harms that are occurring or likely to emerge. A market study by the Australian Competition and Consumer Commission (**ACCC**) would be one way to build a deeper understanding of the current landscape and issues. This would provide the Government with sufficient information to properly consider whether there are specific harms or serious risks that need to be addressed through additional regulation. While the terms of reference for the Digital Platform Services Inquiry appear broad enough to capture some AI applications (for example, AI used in general search services or social media),[70] a market study covering the broader AI sector, that does not require the ACCC to gather information and produce a report within a six-month timeframe, would be preferable in this context.

[70] *Competition and Consumer (Price Inquiry— Digital Platforms) Direction 2020* (Cth).

136. Any additional regulations to address consumer (or competition) issues arising from AI, should be carefully consider the existing and emerging regulatory landscape to ensure consistency and avoid duplication or fragmentation of regulation.

137. For example:

    (a) The Government is continuing to explore multiple law reform proposals and other initiatives that have overlapping implications and relevance to the digital economy, including digital platform rules proposed by the ACCC, the exposure draft of the *Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill* (**Misinformation Bill**—discussed further below), broader consultation on the implementation of an economy-wide prohibition against unfair trading practices, and Government initiatives in relation to Digital Identity. Other Government initiatives relevant to AI are outlined in Attachment A of the Discussion Paper.

    (b) The Government is yet to release its response to the ACCC's digital platform regulation recommendations. If the Government adopts the ACCC's recommendations, there may be scope to consider the application of any digital platform regulatory framework to AI applications.

    (c) The Government is currently consulting on the Misinformation Bill, which contains a broad definition of digital platforms that could cover AI services. The Bill enables the Minister to, by legislative instrument, upon consultation with the ACMA, specify the addition of a new subcategory of digital platform service.

    (d) The Government consulted on options aimed at improving the effectiveness of the consumer guarantee and supplier indemnification provisions under the ACL between December 2021 and February 2022. The consumer guarantee monetary thresholds were increased from $40,000 to $100,000, among other changes. The ACCC is advocating for the ACL to be amended further to enhance the consumer guarantees protections—relevantly, to make it a contravention of the law:

        (i) for businesses to fail to provide a remedy for consumer guarantees failures, when they are legally required to do so, and

        (ii) for manufacturers to fail to reimburse suppliers for consumer guarantees failures that the manufacturers are responsible for.

138. Noting the above examples, a concerted effort is critical to avoid fragmentation in the various Australian reform processes to reduce uncertainty and unintended consequences for those subject to multiple regulatory frameworks. The Law Council is of the view that a complementary and holistic approach is important for improving transparency for consumers and small businesses as well as for regulatory consistency.

How will the law treat erroneous outputs?

139. The Discussion Paper notes that inaccuracies from AI models can 'create many problems'.[71] The listed examples include unwanted bias and misleading or entirely erroneous outputs. The latter example warrants further consideration due to some relevant legal frameworks and principles seemingly being inadequate to address such instances.

140. The Law Council provides the following example to demonstrate the current uncertainty in this regard:

> *Assume, for example, that you enter into a motor vehicle insurance policy with an insurer. The insurer does not deal with you directly but rather through its website, where you have the option of selecting from a range of policies. Once you make a selection, the insurer generates an autonomous smart contract (comprising the chosen policy) and automates its performance through a blockchain network. Your premiums are paid in cryptocurrency out of your digital wallet, rather than a traditional nominated bank account. The smart contract is coded with complex algorithmic processing capacity. Based on your input on the proposal form, it is able to develop a risk profile for you and determine what your premium and other conditions should be (if any). You will be offered insurance if you are deemed a 'reliable driver'. Now assume that the software underpinning the smart contract determines that you are a 'reliable driver', not on the basis of your driving history but on the basis, for example, of your social or professional achievements (which it has discovered through an internet trawl). In other words, the AI-driven smart contract has determined that you are a reliable driver where a human insurance agent conducting a more nuanced assessment would not have done so.*
>
> *Could the insurer claim that the AI-driven smart contract had made a 'mistake' and that the mistake doctrine in contract law applied so as to deny the enforceability of the insurance agreement? The answer is legally unclear. It is not certain if the mistake doctrine could apply because the parties have not been 'mistaken' in the truest sense as to the intended effect of their accord. The smart contract was coded to make decisions and did so. The fact the decision is unintended by the insurer, entirely undesirable, and irrational in the sense that no rational human actor would have made the same decision through the organically intuitive human decision-making process is ostensibly irrelevant under the various existing categories of legal 'mistake'. This result seems absurd given no reasonable insurer would ever have meant to offer insurance to an untrustworthy party. There are significant doubts as to how the mistake doctrine could address the actions of errant AI technologies such as this.*[72]

141. To the extent that AI technologies constitute computer software, they would be recognised as 'goods' for the purposes of the ACL, as the definition of goods under the ACL expressly extends to computer software. The position, however, is less certain for Sale of Goods legislation enacted in the states and territories, where 'goods' do not expressly extend to computer software. For example, there is NSW

[71] Discussion Paper, 7.
[72] See Mark Giancaspro, '"I, Contract": Evaluating the Mistake Doctrine's Application Where Autonomous Smart Contracts Make "Bad" Decisions' (2022) 45(1) *Campbell Law Review* 53.

Supreme Court authority suggesting that software is not a good, under the *Sale of Goods Act 1923* (NSW), if in the form of an intangible download.[73] Where, however, the good is packaged in a storage device of some kind, it could constitute a good.[74] It is conventional for AI software to be sold and distributed through websites or via downloads. While it is likely that downloadable AI software is a 'good' for the purposes of the ACL, it is questionable whether such software would fall within the ambit of state and territory Sale of Goods legislation.

142. There is significant merit in the Government clarifying the boundaries of liability in the foregoing situations and others where AI technologies do not perform as anticipated and loss results.

Competition law issues

143. Widespread access to AI tools has the potential to increase innovation and competition in many markets, including by Australian and international firms. This is especially important in a local context, where Australia has been described by the OECD as performing poorly in its use of data-driven tools, such as AI and data analytics.[75] However, the level of regulation imposed in respect of AI tools can itself affect competition and, in turn, outcomes in markets.

144. It is important to note the distinction between innovation in AI tools and innovation using AI tools. Innovation in AI tools refers to the development and improvement of the actual AI technologies, algorithms, and frameworks. On the other hand, innovation using AI tools refers to the creative and novel applications of existing AI technologies in various industries and sectors.

145. Most directly, regulation of the use of AI tools can affect innovation and competition across the economy, because firms may face limitations and constraints in deploying AI technologies to enhance their products, services, and processes. Stricter regulations may increase the cost and complexity of implementing AI tools, making it more challenging for firms to adopt them effectively. Consequently, firms may be less certain of generating a return on investment from innovative application of AI tools, and therefore may be less incentivised to invest. Australian businesses, in particular, may accordingly find it more difficult to compete internationally if Australian-specific regulation puts them at a relative disadvantage to international firms.

146. Regulation introduced in respect of AI tools is likely to include some fixed cost imposed on firms (that is, a cost that does not vary with output). To the extent that these fixed costs become sunk, they can represent a barrier to entry to new firms. Large incumbent firms may have a greater ability to recover those fixed costs over a larger range of output. In other words, larger incumbent firms may be favoured by a larger regulatory burden. This effect would be compounded if Australia adopted a significantly different regulatory framework than those being developed internationally, especially because product innovation implemented by Australian businesses tends to rely on diffusion of knowledge and technology (as opposed to new-to-the-world, novel innovation).[76]

[73] See, eg, *Gammasonics Institute v Comrad Medical Systems* [2010] NSWSC 267.
[74] See, eg, *Toby Constructions Products v Computer Bar Sales* (1983) 2 NSWLR 48.
[75] See, eg, Productivity Commission, *Advancing Prosperity: 5-year Productivity Inquiry report* (17 March 2023) vol 2, 51.
[76] Productivity Commission, *Advancing Prosperity: 5-year Productivity Inquiry report* (17 March 2023) vol 5, 8.

147. A reduction in competition resulting from a large or discriminatory regulatory burden would be consistent with a reduction in welfare-enhancing innovation, as firms jockey to compete with each other. Ultimately, striking a balance between an appropriate level of regulation and its effect on innovation and competition is important for enhancing the welfare of Australians. Different scales of regulation could assist with striking an appropriate balance although the risks with creating an uneven playing field would need to be considered. The Productivity Commission notes that innovations with lower risks of harm can benefit from 'regulatory sandboxes', whereas more complex systems that may have greater risks of harm can benefit from advance preparation of detailed regulatory frameworks.[77] This is consistent with the Government's approach of adopting a three-tiered system to classify AI tools as low, medium or high risk. Consistent with Government's guide to policy impact analysis, Government should ensure that it considers impacts on competition, innovation, and consumers when it assesses costs and benefits of regulation.[78]

148. Put simply, the potential benefits to Australian businesses and consumers arising from the application of innovative AI tools (including effects on competition) are significant, and Government should ensure that these benefits are considered when assessing regulatory tools for each aspect of AI.

Other areas for consideration

Increasing public trust in the use of AI

149. The Discussion Paper notes adoption rates of AI across Australia remain relatively low, likely due to low levels of public trust and confidence in AI technologies and systems.[79] Concerns about AI have been intensified by AI being used in violation of human rights (including privacy), where manipulative tactics have been used, or to reinforce discrimination.[80]

150. By way of example, the Robodebt Scheme saw the Australian Department of Human Services (now Services Australia) automate its interaction with Centrelink customers via the PAYG program.[81] The inaccuracies and inequities of the scheme caused a corrosion of public trust in the use of AI, as well as Government and its institutions, and significantly undermined public trust in Government administration.

151. In response to these valid concerns, the Law Council suggests the following initiatives or actions:

    (a) greater transparency regarding the use of AI (including by Government);

    (b) additional regulatory and governance responses; and

    (c) further investment in education and research.

[77] Ibid, 10.
[78] Department of the Prime Minister and Cabinet (Cth), *The Australian Government Guide to Policy Impact Analysis* (17 February 2023).
[79] Discussion Paper, 3.
[80] KPMG Australia and The University of Queensland, *Trust in Artificial Intelligence: Australian Insights* (Report, October 2020) 2.
[81] *Royal Commission into the Robodebt Scheme* (Final Report, July 2023).

152. In addition to regulatory initiatives, the Law Council highlights the necessity of education to encourage trust and as a risk mitigation strategy to support responsible AI use and development in Australia.

153. Public engagement forums which facilitate dialogue between AI experts and the public in an easy-to-understand way may assist. Information campaigns, public lectures, and partnerships with schools and universities could also be used. An educational approach will produce a more informed public, better able to understand and participate in discussions about AI and its ethical use.

Ethical responsibilities and AI software testing

154. There are three main actors in the use of AI:

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

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

156. Some contributors to this submission have suggested there should be a gatekeeper approach before AI software is released. The Law Council understands that AI often 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.

157. At the launch of the Robodebt scheme, the system already had demonstrated signs of inadequacy.[82] While the automated system displayed a litany of inaccuracies in its limited release stage in July 2016, the Scheme was fully rolled out in September 2016 'although no proper evaluation of the pilot or manual program had taken place and there were a number of unresolved problems'.[83] The Robodebt scheme exposes the dangers of poorly designed automation, and failure to amend automation errors in the early stages of the process.

158. The car industry provides a useful analogy and potential template for AI pre-release: vehicles are not released to the public until there has been extensive design, testing and approvals. Based on this model, consideration could be given to requiring AI technology and software to 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. However, for this to be effective, there needs to be a clear understanding as to what AI software comprises. It is important to emphasise that a highly specialist and independent entity would be required to devise and administer any testing regime.

Privacy

159. In considering the further development of Australia's privacy laws, compared to that of the European General Data Protection Regulation (**GDPR**), it is important to note that Australia does not have a federal Bill of Rights to support the jurisprudence that

[82] *Royal Commission into the Robodebt Scheme* (Final Report, July 2023) vol 2.
[83] *Royal Commission into the Robodebt Scheme* (Final Report, July 2023) vol 2, xxvi.

underlies how the GDPR is interpreted and applied in European courts.[84] The GDPR is given a more extensive and protective application than Australia's privacy laws because European courts give effect to human rights jurisprudence when interpreting the GDPR. Without similar rights-based jurisprudence in Australia, it is particularly important that Australian governments and their agencies are demonstrably data trustworthy, and remain accountable for the data they collect, use, disclose and process.

160. In the Law Council's view, risk management and any assessment developed as part of the proposed framework should consider existing requirements and processes under the Privacy Act, such as privacy impact assessments. Such considerations are important from the perspective of a co-ordinated and holistic regulatory approach and will assist in limiting the compliance burden on organisations. A sensible approach to AI regulation is to ask whether rules that restrict or prohibit particular uses of AI, or that mandate application of a particular risk assessment framework or methodology, are justified, or whether detect and respond incentives are sufficient to cause appropriate mitigation of risks by regulated entities.

Supporting compliance by small to medium enterprises

161. The Law Council acknowledges that, depending on the regulatory approach, introducing regulation of AI could impact innovation, particularly for small to medium enterprises (**SMEs**). Any regulatory approach must avoid duplication, be consistent and proportionate, and provide clear guidance and support for compliance to SMEs.

162. The Law Council supports education and other tools to encourage and facilitate compliance. 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.

163. Examples of tools to support positive business practices from the National AI Centre and Singapore are outlined in the Discussion Paper.[85] The model contractual clauses published by the European Commission for data transfers between EU and non-EU countries are another example of a tool that could warrant consideration for the Australian context.

164. As discussed, the Law Council supports more general education for the public with respect to AI.

Infrastructure and AI

165. Use of AI in the operation of infrastructure is likely to grow significantly in coming years. This will require wide-reaching safeguards, especially for critical infrastructure. Current critical infrastructure legislation does not, in the Law Council's view, sufficiently address the operation of AI.

---

[84] *Regulation (EU) No 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)* [2016] OJ L 119/1 ('*GDPR*').
[85] Discussion Paper, 15, 24.

Consideration of intellectual property

166. The Discussion Paper expressly states it will not consider intellectual property, particularly copyright. The Discussion Paper says copyright issues will be separately discussed at a 'Ministerial Roundtable on Copyright' forum established by the Attorney-General. The Law Council understands AI will be addressed in the next roundtable discussion in late August 2023.

167. For present purposes, the Law Council notes there are a number of important issues in relation to the intellectual property implications of AI. Generative AI is created through significant data input. LLMs are trained on the basis of enormous volumes of text and MFMs are trained on equally voluminous quantities of data, not limited to text but also including images and speech. To date, there has been no detailed policy consideration of these intellectual property issues, including considerations in connection with the use of copyright. Resolving these issues is critical for stakeholders involved in the process. The Law Council urges expeditious consideration of these intellectual property issues and looks forward to contributing to that process.

Justice system and the legal sector

168. Apart from automated transcription services, the Law Council does not support the use of ADM and AI processes in Australian courtrooms or the justice system more broadly, particularly where it would limit judicial discretion. The Law Council is concerned that, if used ADM processes which rely on factors derived from historic data to predict future outcomes would raise serious issues for the entitlement to due process and compromise judgments predicated on the overall circumstances of the case. ADM processes are inappropriate for use in relation to decisions which could have a significant effect on individual liberties and freedoms.

169. Members of the legal profession have queried whether there is a need for a specific framework encompassing ethical standards and other professional obligations, and 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. However, reliance on AI tools in legal practice does not diminish the professional judgment a legal practitioner is expected to bring to a client's matter. It has been 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 so as not to diminish the quality of legal services. The Law Council and its Constituent Bodies have an important role to perform in setting appropriate standards and providing guidance to the legal profession.