DISCUSSION PAPER

Response from Law Squared

Safe and responsible AI in Australia

LAW SQUARED

Contents

Executive Summary

Law Squared welcomes the opportunity to contribute to the Department of Industry, Science and Resources (**DISR**) *Safe and responsible AI in Australia* discussion paper (the **Discussion Paper**). The Discussion Paper is a significant opportunity to contribute to Government policy regarding Artificial Intelligence (**AI**) use in Australia.

Law Squared has reviewed the Discussion Paper thoroughly and the associated questions proposed by the DISR. We have provided responses to most, but not all, of the questions where our expertise and experience can be of value to the DISR.

Law Squared considers that regulatory action should be taken on AI to ensure the promised benefits of the technology are realised by all and without compromising the rights, safety or security of individuals. The lessens of previous technological advancements should be harnessed to position Australia as a world leader in safe and responsible AI development and use.

Law Squared looks forward to continued engagement on this important issue as the Government's position evolves.

Background - Introducing Law Squared

Law Squared is a global leading Human Centred Law firm, founded in 2016 to provide a true alternative to traditional law firms - for clients and lawyers alike.

To meet the needs of General Counsel, their in-house teams, and business leaders, our mission is to seamlessly bridge the gap between legal expertise and commercial impact.

Our highly skilled lawyers focus on those areas critical to business success, including Corporate + Commercial, Employment + Workplace Relations, Disputes + Litigation, and Digital + Innovation, working as an invaluable extension of the in-house team, or on an ad hoc basis.

Law Squared works exclusively on an upfront, fixed-fee model, prioritising client success over billable hours and ensuring transparency and strategic control over legal spend.

When it comes to selecting a legal partner, reputation matters. Law Squared boasts an unrivalled track record and is widely recognised for our commitment to advancing the legal profession for the better.

With offices in Melbourne, Sydney, Brisbane, and London, Law Squared offers a comprehensive, cost-effective proposition for multinational, ASX-listed, and scaling businesses, or those seeking dual jurisdictional or market-entry support in Australia and/or the UK.

Question 3

Are there any further non-regulatory initiatives the Australian Government could implement to support responsible AI practices in Australia? Please describe these and their benefits or impacts.

1. Non-regulatory initiatives can fill important gaps left by regulatory initiatives in relation to behaviours and actions, and also allow organisations to demonstrate higher levels of compliance or excellence.

2. The key issue to consider is whether there are any particular benefits that further non-regulatory initiatives would cover that are not addressed, or not sufficiently addressed, by the proposed non-regulatory initiatives in the Discussion Paper.

3. We consider that the non-regulatory initiatives considered by the Australian Government in the Discussion Paper are relatively comprehensive. We encourage the Australian Government to focus on a few non-regulatory mechanisms in the first instance to increase public confidence in AI, and to allow organisations to demonstrate compliance.

4. The main limitation for voluntary measures is that there is likely to be limited uptake of these voluntary measures, as it is often the organisations with more resources that tend to take up voluntary measures. Small and medium enterprises (**SMEs**) and not-for-profits (**NFPs**) often cite resourcing as an issue for compliance with voluntary mechanisms. The benefits of voluntary measures are generally that they are good for increasing public and corporate consumer trust, and are useful for demonstrating particular excellence or safety with a product or service.

5. We consider that some of these initial initiatives may be voluntary technical standards, public education and awareness, voluntary ethical principles, and voluntary accreditation:

Voluntary technical standards

6. We consider voluntary technical standards to be a useful mechanism to increase confidence in private and public sector use of AI. In our experience, a common example of a voluntary standard that increases consumer confidence in private and public sector organisations ISO/IEC 27001 – Information Security Management Standard (**ISO 27001**). ISO 27001 is very likely to also be applicable to many AI providers and may be a voluntary standard that the Australian Government could recommend to AI providers to align or comply with.

7. A limitation for this recommendation is that ISO 27001 compliance is generally expensive and more achievable for larger organisations, and less so for smaller organisations. This is likely to be a limitation for any voluntary technical standard.

Public education and awareness

8. This could be accomplished by Government publishing information that is accessible to Australian individuals who are not well versed in AI and technology, by television campaigns, and by Government policy statements. The benefits of this approach are that these measures should be accessible and easily understandable by most of the

Australian population, the limitation of this approach is that significant government resources may be expended in accomplishing this measure;

Voluntary ethical principles

9. These are already being adopted by some private and public organisations to increase public and customer trust in the organisation's use of AI,[1] and we anticipate will continue to be an important mechanism for organisations to demonstrate their responsible use of AI. A consideration for the Australian Government is to have different ethical principles for different levels of risk in relation to the use of the AI. This will allow organisations to be able to comply with the ethical principles which best suit the circumstances; and

Voluntary accreditation

10. Similar to the voluntary technical standards and for similar reasons, we consider that voluntary accreditation regimes will be a helpful mechanism to increase public and corporate confidence in the use of AI.

Question 5

Are there any governance measures being taken or considered by other countries (including any not discussed in this paper) that are relevant, adaptable and desirable for Australia?

11. Australia's current legislative framework for technology has a broad scope and does not specifically contemplate AI. Whilst the current regime is robust its technology neutral basis creates gaps. This issue is not unique to Australia and has been considered globally as countries scramble to regulate this fast-moving technology.

12. The approach to regulation has differed around the world from a highly controlled approach adopted by China to a light self-regulating sector specific approach taken in Singapore. Australia must decide on an approach which strikes a balance between winning public trust and fostering innovation and the continued development and deployment of AI.

13. Australia has an existing framework which regulates technology. This is achieved through sector specific regulations for areas which overlap into technology such as privacy and data protection. As AI evolves it challenges this framework and brings forward new risks which fall outside the existing regulatory regime. For example, the exponential growth of AI means organisations lack the tools, guidance and experience to confidently deploy AI in pace with its development.

14. Australia has the advantage of looking to other countries who are further ahead in regulating AI. Some countries have relied on existing regulations to govern AI whilst and others are creating new regulations for an essentially uncharted area.

15. A risk-based approach has been favoured globally with regions such as the EU imposing complete bans on certain activities which pose an unacceptable risk through to requiring minimal regulation for low-risk activities.

1 *Australian Government, Department of Industry, Science and Resources, "Safe and responsible AI in Australia", Discussion Paper (June 2023), p 14.*

16. Countries around the world are grappling with the best way to regulate AI with a view to curtailing the potential harm AI can cause and fulfilling ambitions to be world class hubs for AI which has immense economic advantage. [2]

17. After examining several approaches taken around the world, the UK and EU approaches will be considered in this response, based upon the fact the EU and UK are quite far ahead in the regulation of AI and the approaches could potentially be effectively implemented in Australia.

United Kingdom

18. In Australia AI has the potential to impact several sectors. These impacts are likely to be unique to that sector creating gaps with current legislation, therefore, considering the sector specific approach taken by the UK may address any gaps created by the regime in Australia.

19. The UK approach has several advantages. This approach is flexible and allows regulators to respond based upon their expertise and new technological development for that sector. For example, data protection regulators can ensure AI is used in such a way as to protect personal information. This requires an intimate understanding of data protection, and the way AI uses personal data and, in some cases, generates personal data. Data protection regulation has the potential to govern AI in a way which garners public trust, something which is currently lacking in Australia.

20. Whilst the UK approach does have it merits there are issues which should be considered. Some include possible contradictions and incoherence in relation to guidelines. There is also the risk of issues spanning over more than one regulator. The view taken in the Vallance Report of a collaborative approach is a likely solution "the best way to regulate digital emerging technologies would be to work with regulators and develop a multi-regulator sandbox in order to foster collaboration". [3]

21. The UK have taken a delicate approach when it comes to implementing guidelines, where regulators will provide industries with guidance on how to implement and manage AI responsibly and ethically. This stance is more likely to foster innovation and development of AI and attract the interests of organisations who might otherwise shy away from AI regulation until they are forced to do so.

European Union

22. The EU has adopted a more robust approach and will impose new laws drafted specifically for AI. Australia could benefit by this approach given the guidelines will be tailored specifically for AI and will be statutory, legally binding and enforceable. Business will have a concrete incentive to comply and will not have the option to ignore the need to manage AI responsibly and ethically.

23. The certainty created by this approach is appealing and Australia would benefit from the legal certainty. However, this approach also has issues. The general landscape of AI is still very uncertain. Accordingly, there are likely to be unknown risks which will be very difficult to anticipate, so legal certainty may not be possible at this stage. It is evident regulations needs to be agile and this has already been demonstrated by the EU who have already made changes to the draft legislation.

---

2 *'Pro-innovation approach to AI' UK White Paper on AI (22 June 2023).*

3 *Pro-innovation Regulation of Technologies Review' Vallance Report – Sir Patrick Vallance.*

24. Australia currently has a voluntary principled approach to AI. The principled approach would benefit other countries as it aims to counter any social issues caused by AI and uphold ethical practices. Australia has taken on a human centred approach which in some ways mirrors the approach encouraged by the UN and the OECD with a goal of ensuring a minimum guarantee for all. This approach provides an opportunity to improve the public perception of AI.

25. Given the need for agility and flexibility when it comes to regulating AI, the sector specific approach taken by the UK is preferred. Working collaboratively with industry experts to tackle unique issues related to AI deployment would be difficult if the general top-down approach adopted by the EU was implemented. Unique and unforeseen issues are likely inevitable, and these should be taken into account when deciding on an approach for Australia.

Question 6

Should different approaches apply to public and private sector use of AI technologies? If so, how should the approaches differ?

26. Law Squared does not consider that different regulatory approaches are appropriate for public and private sector use of AI technologies. Differentiating regulatory approaches on the basis of public versus private sectors results in slower adoption of regulatory standards and worse outcomes for individuals.

27. We have seen different approaches for the public and private sectors play out regarding the use of Privacy Impact Assessments (**PIAs**) under the Privacy (Australian Government Agencies – Governance) APP Code 2017 (the **Code**). The Code requires Agencies under the Privacy Act 1988 (Cth) (**Privacy Act**) to conduct a PIA for all high privacy risk projects. There is no similar requirement on the private sector. This has led to the private sector predominantly not undertaking PIAs for high-risk projects and in turn continues to lead to slower adoption of good privacy practices.

28. It may be appropriate to implement additional sectoral regulation for some sectors, as has been done for critical infrastructure with the Security of Critical Infrastructure Act 2018 (Cth). However, any sectoral regulation should be in addition to the baseline regulatory regime that must apply to the public and private sectors equally.

Question 9

Given the importance of transparency across the AI lifecycle, please share your thoughts on: (a) where and when transparency will be most critical and valuable to mitigate potential AI risks and to improve public trust and confidence in AI?

29. At Law Squared, we firmly believe that to improve public trust and confidence in AI, transparency measures must go beyond disclosure. Meaningful engagement with stakeholders, including affected communities, experts, and regulatory bodies, is essential. Establishing mechanisms for inclusive consultations (including with employees), public input, and ongoing dialogue can facilitate the development of

ethical guidelines and policies, address concerns, and ensure that AI systems align with societal values.

30. Transparency plays a critical role at the following stages of the AI lifecycle: Development and Deployment, High-risk areas, Data Governance and Privacy.

Development and deployment

31. During the development and deployment phases, transparency is crucial in establishing accountability and trustworthiness. Organisations should provide clear and comprehensive documentation detailing the design, training data sources, algorithmic decision-making processes, and any potential limitations or biases of AI systems.

32. This transparency enables thorough scrutiny, identification of potential risks, biases, or discriminatory outcomes, and facilitates timely remediation. By way of example, development teams must consider is their AI system in any way unlawfully discriminates (directly or indirectly) on the basis of one or more protected attributes as set out in Australia's federal and State/Territory discrimination legislation (for example Disability Discrimination Act 1992 (Cth), Equal Opportunity Act 2010 (Vic) etc.), and if so, how it will be fixed? Such considerations should be documented in formal risk assessments and made available to the public.

33. We note that algorithmic bias was a key focus of the Australian Human Rights Commission's Human Rights and Technology Report in 2021[4] and examples of discrimination against individuals by AI systems in the past have included:

    a. racial discrimination which disproportionately targets minority groups; [5]
    b. gender discrimination;[6] and
    c. socio-economic discrimination.[7]

34. One way to avoid repeating these mistakes and fostering an environment where anti-discriminatory design can flourish is to publish AI risk assessments. Public disclosure of relevant details will foster transparency, promote responsible AI practices, and reduce the risk of unintended consequences.

35. We accept that there will likely be a reluctance to publish commercial sensitive information related to the risks posed by a particular AI system. This is where Government can play a key role by taking the lead in undertaking AI risk assessments and publishing those assessments for public consumption in combination with enforcing mandatory requirements discussed elsewhere in this response.

High-risk areas

36. Transparency is of utmost importance in AI systems deployed in sensitive and high-risk domains such as healthcare, criminal justice, and financial services. In these contexts, individuals' lives and fundamental rights can be significantly impacted by AI decisions. Ensuring transparency about the algorithms, methodologies, and underlying data used in AI decision-making processes is crucial.

---

4 *Australian Human Rights Commission's Human Rights and Technology Final Report (2021), Chapter 8.*
5 *K Hao, 'AI is sending people to jail - and getting it wrong', MIT Technology Review website, 21 January 2019*
6 *C Hanrahan, 'Job recruitment algorithms can amplify unconscious bias favouring men, new research finds', ABC News website, 2 December 2020.*
7 *D Kolkman, 'What the world can learn from the UK's A-level grading fiasco', LSE Impact Blog, 26 August 2020.*

37. Transparency allows affected individuals to understand the basis for decisions that have a significant effect on their lives, such as available health care or financial services. Without this transparency we risk creating a situation we have seen play out in the privacy sphere whereby, until recently, individuals do not know what their personal information is being used for or who it may be disclosed to. Like privacy, the key to public trust is providing individuals with choice about how they engage with AI.

38. Equally important is ensuring information provided to individual's is accessible, i.e. written in plain language that most people can understand. The recent push by regulators worldwide to make legislative guidance accessible for businesses and individuals should continue for AI. AI material should include practical guidance and guides from Government to assist businesses with implementation of AI and individuals with understanding AI.

Data Governance and Privacy

39. Transparent data governance practices are vital to address concerns related to privacy, data protection, and security throughout the AI lifecycle. Organisations should be transparent (including but not limited to their privacy policies) about data collection, storage, sharing, and usage practices. Individuals should be informed about the types of data collected, purposes of collection, and any third parties with whom the data may be shared. Transparent data governance helps build trust by demonstrating that organisations prioritise privacy protection and comply with relevant data protection laws and regulations.

Question 10

Do you have suggestions for: (a) whether any high-risk AI applications or technologies should be banned completely?

40. While the regulation of AI remains in an early state globally, there is a developing international direction towards a 'risk-based' approach for governance of AI. We have seen steps taken by other countries such as Canada and New Zealand who have decided to impose requirements for their public sectors to take action on this front.

41. Law Squared considers that a principle based approach is to be preferred to ensure that legislation and regulation is able to keep pace with AI development. The Canadian *Directive on Automated Decision-Making* (**DADM**) is an example of this approach.

42. The DADM classifies the impact AI technologies can have into four categories:

    a. Low ('level I') risk: impacts of which are reversible or for a short time.
    b. Moderate ('level II') risk: impacts of which are likely reversible and short-term.
    c. High ('level III') risk: impacts that can be difficult to reverse and that might be ongoing.
    d. Very high ('level IV) risk: impacts of which are irreversible and perpetual.

43. To determine the impact level of an AI technology, an Algorithmic Impact Assessment (**AIA**) must be conducted which contains 51 risk and 34 mitigation questions, and scores obtained are based on factors such as system's design, algorithm, decision type, impact and data available.[8]

44. We believe that use cases that fall within the 'High' or 'Very high' category should be banned. Whilst one should not disallow something purely because it's 'risky', in the case of AI technology, especially at the 'High' or 'Very High' level, the consequences that may arise can have lasting and detrimental impacts on individual's lives.

45. We also agree with the approach taken by the European Union in terms of examples of what is classified as 'high' or 'unacceptable risk'. This table was attached as Attachment B to the Discussion Paper. An approach could be adopted that is guided by the Canadian and EU approaches.

Question 11

What initiatives or government action can increase public trust in AI deployment to encourage more people to use AI?

46. The Discussion Paper identifies one of the factors influencing the adoption of AI being the low levels of public trust and confidence of Australians in AI technologies and systems,[9] and considers the introduction of formal regulatory responses in relation to the use of AI, as well as non-regulatory mechanisms.[10]

47. The key issues for the Australian Government in relation to increasing the public's trust in AI deployment and increasing the use of AI are:

    a. utilising the appropriate mechanisms to ensure that private and public sector organisations are using AI responsibly; and
    b. decreasing any fear and misunderstanding of AI in the public.

Taking a regulatory approach

48. Our position is that protecting Australian individuals and private and public sector organisations will be best done by the Australian Government pursuing regulatory initiatives, particularly against the challenges and risks identified in the Discussion Paper such as lack of public trust in AI, generation of deepfakes to cause deceit, creating misinformation and disinformation, encouraging people to self-harm, and inaccuracies from AI models.[11]

49. We recommend that regulatory initiatives take the form of a specific act in relation to the governance of AI, and the supplementary amendment of current legislation where appropriate as set out in our response to question 18.

8 *Algorithmic Impact Assessment Tool, (Webpage, date accessed 4 July 2023) <https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.html>*

9 *Australian Government, Department of Industry, Science and Resources, "Safe and responsible AI in Australia", Discussion Paper (June 2023), page 3, citing Gillespie, N., Lockey, S., Curtis, C., Pool, J., & Akbari, A. (2023) "Trust in Artificial Intelligence: A Global Study" The University of Queensland and KPMG Australia, page 14 (accessed 26 June 2023).*

10 *Australian Government, Department of Industry, Science and Resources, "Safe and responsible AI in Australia", Discussion Paper (June 2023), pages 3, 27 – 30.*

11 *Australian Government, Department of Industry, Science and Resources, "Safe and responsible AI in Australia", Discussion Paper (June 2023), pages 4 and 7.*

50. While the limitations to this approach must be considered, in particular, the requirement that parliament must pass legislation and the time that often takes, we consider that mechanisms can be built into the legislation to allow mandatory codes of practice or other binding legislative instruments to be issued by the regulator(s) or relevant government department(s) on shorter notice such as for particular sectors, types of AI, or applications of AI. We consider that allowing for legislative instruments to be created by the relevant regulator(s) or relevant government department(s) under the relevant legislation will allow greater agility for the regulatory approach, overcoming some of the limitations with the regulatory initiatives, barring the initial Parliamentary passing of the regulatory initiatives.

51. One of the reasons why regulatory initiatives are likely to be the most effective solution to addressing many of the issues is because non-regulatory, and more importantly, non-mandatory initiatives, are unlikely to have a strong effect on private and public sector behaviour across the board. This is because, in our experience, resourcing is often cited as an issue for compliance with voluntary regimes by smaller organisations, such as SMEs and NFPs. Voluntary regimes are more likely to only be taken up by larger organisations with more resources. This is exemplified in the Discussion Paper in relation to the uptake of Australia's AI Ethics Framework by larger organisations, such as Microsoft, Salesforce, Google, and IBM.[12]

52. A couple regulatory mechanisms we consider particularly important to increase public trust in the use of AI mechanisms are:

    a. introducing a right for individuals not to be subject to automated decision making;
    b. requiring organisations to notify individuals that they are using AI in the delivery of their services; and
    c. seeking individuals' consent to the use of AI in relation to the delivery of services to them.

53. We have addressed these further in our response to question 18.

Taking a voluntary approach

54. We consider that voluntary mechanisms will serve as an important supplementary mechanism to uplift public confidence in AI, and will allow organisations to demonstrate particular compliances or industry excellence where they comply with the voluntary standards.

55. We consider that any of the voluntary standards in figure 3 on page 27 of the Discussion Paper would be viable mechanisms to supplement the regulatory framework for AI.

Question 12

How would banning high-risk activities (like social scoring or facial recognition technology in certain circumstances) impact Australia's tech sector and our trade and exports with other countries?

12 *Australian Government, Department of Industry, Science and Resources, "Safe and responsible AI in Australia", Discussion Paper (June 2023), page 14.*

56. At Law Squared, we believe that there should be a balance struck between protecting individual rights and fostering technological advancement. In our opinion a comprehensive approach that includes robust regulation, transparency, and accountability mechanisms can help mitigate risks while preserving Australia's position as a leader in the global tech sector. Individual rights can be preserved while making technological progress.

57. Banning high-risk activities such as social scoring or facial recognition technology in certain circumstances would have significant implications for Australia's tech sector and its trade and exports with other countries. It is therefore important to consider both the potential positive and negative impacts of such a ban.

58. On one hand, banning high-risk activities can be seen as a proactive measure to protect individual privacy, promote ethical AI practices, and mitigate potential risks associated with these technologies. This could enhance public trust in the use of AI and contribute to a more responsible and accountable tech sector. It may also encourage the development and adoption of alternative technologies that prioritize privacy and security, stimulating innovation and new business opportunities.

59. It is key is to remember that AI is a quickly evolving technology that has the potential to outgrow legislative guardrails. Accordingly, any banned activity list, if implemented, must be able to be updated at a similar speed to which AI evolves.

60. On the other hand, it is crucial to carefully assess the potential negative consequences that a ban may have on Australia's tech sector and international trade and exports, in particular, the impact the negative consequences on the following:

Economic impact

61. The tech sector in Australia has been a driver of economic growth, innovation, and job creation. For example, Australia's technology sector is estimated to be worth around A$167 billion and is the third largest contributor to GDP in the country.[13]

62. Banning high-risk activities could potentially stifle the development and competitiveness of tech companies operating in Australia. It may limit their access to global markets and hinder their ability to compete with companies from countries where these technologies are permitted.

Operational impact

63. High-risk activities can better assist tech sector businesses in carrying out their operations more efficiently. A ban on such high-risk activities can therefore lead to unrealised productivity and revenue. For example, facial recognition can make it easier and more cost-effective for business to ensure that it:

    a. provides a safer workplace for employees by knowing exactly who is in the workplace and when (and hence comply with their duty of care under State/Territory based legislation and common law); and

    b. pays its employees correctly by knowing exactly when and where employees are performing work (and hence comply with their obligations under the Fair Work Act 2009 (Cth), applicable Modern Award etc.)

13 *Australian Government, AusTrade 'Why Australia – Digital Technology' Report (2023).*

Trade relations

64. Banning certain technologies could strain trade relations with countries that have a vested interest in the development, export, or use of these technologies. It may result in trade barriers, restrictions, or retaliation from countries that perceive the ban as an unjustified impediment to trade. This could have a negative impact on Australia's export industry and its ability to collaborate with international partners in the tech sector.

65. We have seen such international inconsistencies play out since the introduction of the EU's General Data Protection Regulation (**GDPR**) in 2018. In creating 'best-in-class' privacy protections for its citizens, the EU created a commercial barrier for other nations seeking to trade with the EU. Accordingly, the impact of any regulatory or non-regulatory approach should be considered in the context of Australia's international strategic and trade priorities to avoid unnecessary or unintended barriers.

Technological advancement

66. Prohibiting high-risk activities outright may impede the opportunity for Australian researchers, innovators, and tech companies to develop and refine these technologies responsibly. By implementing stringent regulations and oversight frameworks instead of a complete ban, Australia could strike a balance between fostering innovation and addressing potential risks associated with these technologies.

67. Accordingly, and as discussed below in a response to question 17, a tiered approach to regulation should be considered so as to impose different requirements on AI development and AI consumption. Such an approach could foster a safe environment where high-risk activities can be researched, developed and de-risked before commercialisation and consumption.

International harmonisation

68. The ban on high-risk activities may also complicate efforts to establish international standards and regulations governing AI and emerging technologies. Australia's ability to participate in global discussions and shape international norms could be impacted if it is seen as taking an extreme approach by outright banning certain technologies. Collaborative efforts with other countries to establish responsible practices and ethical guidelines could be hindered as a result.

Question 14

Do you support a risk-based approach for addressing potential AI risks? If not, is there a better approach?

69. Law Squared supports a risk-based approach that incorporates ethical considerations, promotes stakeholder engagement, and fosters continuous evaluation and learning. This will ensure that the approach remains effective, proportionate, and responsive to the evolving landscape of AI technologies and associated risks.

70. A risk-based approach (like the approach used in Canada and the EU)[14] allows for a nuanced and tailored response to the unique challenges posed by AI technologies,

14 *Government of Canada, 'Directive on Automated Decision-Making', Government of Canada website, 25 March 2023.*

taking into account their specific applications and potential consequences, and therefore it is preferred.

71. The advantages of a risk-based approach include flexibility, proportionality and responsiveness.

Flexibility

72. A risk-based approach allows for adaptability and agility in addressing AI risks. It recognises that not all AI systems pose the same level of risk and avoids applying a one-size-fits-all regulatory framework. Instead, it enables regulators to prioritise resources and interventions where they are most needed, targeting high-risk areas while minimising unnecessary burden on low-risk applications.

Proportionality

73. The risk-based approach ensures that regulatory interventions are proportionate to the potential harm posed by AI systems. It avoids stifling innovation and imposing excessive compliance burdens on low-risk applications. By focusing on high-risk areas, it allows for the development and deployment of AI technologies that have demonstrable benefits while effectively managing potential risks.

Responsiveness

74. The risk-based approach recognises that the AI landscape is evolving rapidly, with new technologies and applications emerging continuously. It enables regulators to monitor and reassess risks regularly, adapting regulatory measures to keep pace with technological advancements and emerging concerns. This responsiveness ensures that regulatory frameworks remain effective and relevant in addressing evolving AI risks.

75. While Law Squared supports a risk-based approach over alternatives, it is essential to acknowledge that it should be complemented by other key considerations.

Ethical considerations

76. A risk-based approach should not neglect ethical concerns associated with AI technologies. Ethical considerations such as fairness, transparency, and accountability should be integrated into the risk assessment process to ensure that potential risks are evaluated comprehensively.

Public input and stakeholder engagement

77. The perspectives and insights of various stakeholders, including affected communities, experts, and human rights organisations, should be considered in the risk assessment and regulatory decision-making processes. Meaningful public input and engagement help ensure that the risks and benefits of AI technologies are assessed holistically and that regulatory measures are well-informed and inclusive.

Continuous evaluation and learning

78. A risk-based approach should be accompanied by ongoing evaluation and learning to assess the effectiveness of regulatory measures and identify emerging risks. Regular

review and adjustment of regulatory frameworks based on lessons learned and technological advancements are essential to maintain a robust and adaptive approach to AI risks.

Question 15

What do you see as the main benefits or limitations of a risk-based approach? How can any limitations be overcome?

79. Law Squared considers there to be benefit and limitations to a risk-based approach to AI. These benefits and limitations arise due to the fundamental intersection of new technology and existing individual rights. We consider that these interests can be complementary rather than competitive provided a risk-based approach reflects broader society values and norms.

Benefits

80. In our experience, the benefits of a risk-based approach are that it:

    a. sets out a framework for public and private sector organisations to consider and assess the risks of a particular activity;

    b. may set out or clearly implicate the appropriate course(s) of action in accordance with the level of risk identified in the activity;

    c. encourages proactive action and engagement by public and private sector organisations with the risks of an activity;

    d. encourages accountability in organisations to identify, categorise and mitigate risks; and

    e. is a useful approach which has previously been used in relation to new technologies.

81. Examples of measures of this nature include:

    a. a.PIAs under the Privacy Act. A PIA is a systematic assessment of a project to identify the positive and negative impacts that project might have on the privacy of individuals. A PIA will make recommendations for managing, minimising or removing negative impacts impact,[15] as required under Australian Privacy Principle 1 and section 33D of the Privacy Act.

    b. Data Protection Impact Assessments (**DPIA**) under Article 35 of the EU GDPR. A DPIA requires a data controller (the entity that controls the "when" and "how" of data processing) to assess the impact new ways of handling personal information may have on individuals. Key to these assessments is considering the nature, scope, context and purposes of that handling, and whether it is likely to result in a high risk to individuals' rights.

15 *Office of the Australian Information Commissioner, Australian Government, "Guide to undertaking privacy impact assessments" (2 September 2021), accessed 24 June 2023.*

82. While an initial threshold assessment is often required prior to engaging in a full PIA or a DPIA, the assessment of the risks to individuals in the project is built in early for organisations, increasing their engagement and accountability in the process.

83. We consider that PIAs and DPIAs are a good model for assessing the privacy risks of new projects and technologies. A requirement for a similar assessment for AI technologies should be strongly considered to assist organisations and consumers adoptions of AI.

Limitations

84. In our experience, the limitations of risk-based approach are that:

    a. it may be applied differently to and by private and public sector organisations. For example, there is only a mandatory legal requirement for government agencies to conduct a PIA under the Privacy Act, and no mandatory requirement for private sector organisations to do so. This means that private sector organisations are much less likely to conduct PIAs;

    b. there is a reliance on organisations to be accountable to deciding whether it is appropriate to conduct a risk assessment in some circumstances, which can be overlooked or not fully completed where resourcing is an issue, such as for SMEs and NFPs; and

    c. grey areas will be open to interpretation if clear guidance is not provided by regulators.

Overcoming the limitations

85. In our view, the benefits outweigh the limitations in relation to adopting a risk-based approach. This is further supported by other countries taking this approach, most importantly, the EU in its recently passed AI Act.[16] The EU has debatably been the global leader in privacy and technology laws for some period of time, starting with the GDPR, so the Australian Government should strongly consider the benefits of the EU's approach.

86. Ways to overcome the limitations identified above may include:

    a. making any sort of PIA or DPIA analogy for the use of AI mandatory for private and public sector organisations of any size. While this may raise push back from organisations which often cite resources as a barrier to full compliance, the benefits to the Australian people outweigh this issue, and this should be made clear as the priority in any guidance;

    b. having more stringent requirements for larger private or public organisations for any sort of PIA or DPIA analogy for the use of AI, and lesser requirements for SMEs and NFPs to overcome resourcing difficulties. However, this must account for any structuring of corporate groups intended to avoid any size related requirements;

    c. ensuring that the relevant regulator(s) issue guidance on the interpretation

16 *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 (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD))" (14 June 2023), accessed 24 June 2023.*

of the risk-based assessments soon after the passing of any law on AI requiring a risk-based approach and prior to the end of any grace period for the commencement of the regime. Clear and accessible regulatory guidance is likely to increase compliance with it, and reduce the risk of any grey areas being used to the advantage of the organisation.

Question 16

Is a risk-based approach better suited to some sectors, AI applications or organisations than others based on organisation size, AI maturity and resources?

87. Regardless of the sector, the AI applications, size, AI maturity and resources of an organisation, a risk-based approach is a suitable option as it can be tailored dependent on the level of risk as opposed to size, AI maturity or resources. However, the level of risk is likely to increase if an organisation does not have the resources or the experience to implement and deploy AI safely.

88. One of the main challenges with implementing a risk-based approach is trying to access risk for technology which is uncertain and has risks which have not been realised.

89. A risk-based approach is likely to be adopted in Australia if we are to look to the UK and EU models of regulation. Whilst these models are robust, they could lead to inconsistency and inaccuracies in regulating AI in the case of the UK or rigid and ineffective regulation in the case of the EU. For example, assessing the level of risk may mean low risk organisation would have no restrictions whilst high risk organisations could be banned altogether.

90. Historically, some of the most significant risks around AI involve lack of transparency, bias, privacy concerns, ethical dilemmas, security risks, and dependence on AI. Risk also lies in how the AI system is deployed for example deploying AI in the medical sector may pose a higher risk compared to deploying AI in the education sector. Both methods of deployment will differ and present unique risks.

91. There needs to be a high level of multi sector collaboration to tackle AI risks and come up with practical tailored solutions. A sector-based risk approach is well placed to provide an agile and innovation friendly form of regulation. The results of the risk assessments should be fed back to developers, the organisations/sectors and users in order to foster a transparent regime and allow these stakeholders to refine their skills and awareness to identify and anticipate risks.

92. Collaboration between regulators, sectors and developers is paramount for developing an effective risk-based system.

93. While a risk-based approach to AI is a practical solution for regulation, this can be best achieved using a sector-based approach as opposed to a centralised approach using general AI specific legislation. The centralised approach runs the risk of being unyielding and ineffective if applied to a technology which is rapidly evolving. Although the sector-based approach attracts another set of issues such as inconsistencies it appears to be the most logical approach at this time. This risk-based sector approach

will give experts in their field an opportunity to work collaboratively with regulators and developers which will hopefully help to strike a balance between implementing necessary regulation and encouraging innovation, development and ethical practices in relation to AI.

Question 17

What elements should be in a risk-based approach for addressing potential AI risks? Do you support the elements presented in Attachment C?

94. A risk-based approach for addressing potential AI risks should consider, at a minimum, the following elements. Unless where inconsistent with the below, Law Squared supports the elements presented in Attachment C.

Tiered approach to regulation

95. DISR should consider a regulatory separation between AI developing organisations and AI consuming organisations. The difference of developing and consuming AI is material and a risk-based approach needs to be tailored to the specific activity that the organisation is engaging in.

96. Independent AI risk assessments should be required for AI developing organisations. Such assessments should be live documents that are updated as projects project. The current approach to privacy impact assessments under the Privacy Act could be used as a guide here, however appropriate guidance will need to be developed in concert with any regulation.

97. The perception and assessment of risk can vary based on the risk appetite of the organisation or individual. Where the organisation stands to acquire commercial gains through the development and commercialisation of AI or an AI product, there may be a conflict of interest for them to self-assess the risk impact of their AI. This is especially true for smaller, 'agile' businesses who may prioritise speed to market over risk mitigation.

98. AI consuming organisations should be required to review the AI risk assessment of the relevant AI developing organisation, then conduct an independent assessment as to how the AI product will affect their business specifically. There is an inherent conflict of interest between the impact of new technology on a business and the perceived commercial benefit. Further, there is a general lack of understanding amongst adopters as to the full implications of the technology on a business and its customers.

Training

99. Training requirements should also be separated between AI developers and AI consumers. We note:

    a. Attachment C is unclear in its stance on this separation.
    b. Developers of AI should be trained on concepts such as implicit bias, AI risk assessment, and other 'maker' related training modules by an independent body.
    c. Consumers of AI should be trained on concepts such as privacy, data governance, understanding the nuances of AI, and other consumer related training modules.

Remotely disable self-learning AI

100. For medium to high-risk AI types, especially ones that are able to self-learn, there should be either a manual or automated way to remotely disable the AI functionality. Given the nature of certain types of AI, there is a potential for these AIs to self-develop new functionality which increases their risk profile. In such case, the AI should be disabled until a new risk impact assessment is completed, which also considers the AI's ability to self-develop.

Independent regulatory body

101. Given the varying perspectives and interpretations on acceptable risk, an independent regulating body should be considered to provide guidance on acceptable risk practices and enforce compliance of appropriate requirements.

102. This regulatory body must be empowered to regulate the public and private sectors without fear of budgetary or political retribution.

Question 18

How can an AI risk-based approach be incorporated into existing assessment frameworks (like privacy) or risk management processes to streamline and reduce potential duplication?

103. The key issues for the Australian Government in relation to implementing an AI risk-based approach into existing frameworks are:

    a. to ensure that current regulatory frameworks are being used accordingly;
    b. to ensure that the regulatory framework for the use of AI is clear, accessible and able to be understood by public and private sector organisations; and
    c. to avoid duplication.

104. There are several relevant general regulations and sector-specific regulations that are identified in the Discussion Paper.[17] We have addressed the regulations that we consider the most relevant below.

General regulations

105. Overall, we agree that the regulation of AI should be incorporated by the Australian Government into existing frameworks where sensical, and supplemented by a specific AI legislation that deals with AI the development, use and ongoing regulation of AI. The goal should be avoid duplication and to make it easy to understand.

106. One risk of this approach is that it may result in incomplete implementation and compliance by some organisations, particularly with types of organisations which sometimes cite resourcing as an issue in compliance. The fragmented regulation is the hard it tends to be to comply with.

107. We therefore recommend that the Australian Government provides clear resources and non-regulatory frameworks for organisations to increase proper implementation

17 *Australian Government, Department of Industry, Science and Resources, "Safe and responsible AI in Australia", Discussion Paper (June 2023), p 10.*

and understanding of the regulatory framework for AI across all sectors. We consider that this will also increase the trust in the use of AI by the Australian people.

108. We further agree that that approach set out in the Online Safety Act sets a good example for any potential AI act in relation to establishing basic expectations, and providing for the development of new codes to address any new issues. This is likely to be a stronger approach than the development of common law over time as it provides upfront certainty.

109. We have considered several existing regulatory regimes below.

Privacy Act 1988 (Cth)

110. We consider that the Privacy Act will be an important regulatory mechanism through which the Australian Government can address some of the risks of the use of AI in Australia. In particular, the Privacy Act will regulate how private and public sectors collect, use and disclose personal information with AI. Given that the Privacy Act is currently undergoing its own review, there are some specific proposals in that review which are pertinent to the issues raised in this AI consultation.

111. Proposal 19.1 of the Privacy Act Review report recommends that organisations include information in their privacy policy about whether personal information will be used in any automated decision making process which has a legal or similarly significant effect on an individual's rights.[18] Proposal 19.3 of the Privacy Act Review report recommends that individuals are given a right to request how these decisions are made.[19]

112. While we agree that proposals 19.1 and 19.3 of the Privacy Act Review will be important in protecting individuals' rights in relation to the use of AI, we consider that this is not sufficient protection for individuals.

113. We recommend that there should be a new right in the Privacy Act for individuals not to be subject to a decision based solely on automated processing which produces legal effects concerning that individual, or which similarly significantly affects that individual, unless it is necessary for entering into or performing a contract between the individual and the organisation, is authorised by law, or is based on the individual's explicit consent. This right is contained in article 22 of the GDPR, and is particularly relevant to the use of AI in relation to private and public sector organisations' use of AI in their operations.

114. To further protect individuals in relation to the use of AI, we further recommend that, at minimum:

    a. the small business exemption is removed from the Privacy Act, as under proposal 6.1 of the Privacy Act Review report, so as to ensure that any organisation of any size must comply with the requirements of the Privacy Act; [20]

    b. the definition of "consent" in the Privacy Act is amended to require it to be voluntary, informed, current, specific and unambiguous under proposal 11.1 of the Privacy Act Review report; [21]

---

18 *Attorney-General's Department, Australian Government, "Privacy Act Review: Report 2022", (16 February 2023), page 12.*
19 *Ibid, p 12.*
20 *Ibid, p 6.*
21 *Ibid, p 8.*

c. that all APP entities will be required to conduct a PIA for activities with high privacy risks, per proposal 13.1 of the Privacy Act Review report. As set out in our response in question 15, we consider that a requirement to conduct PIAs forms a critical element of any mandated risk-based approach to AI regulation in Australia;[22] and

d. that enhanced risk assessment requirements are mandated for the use of biometric information (such as facial recognition technology), per proposal 13.2 of the Privacy Act Review report.[23]

*Schedule 2 to the Competition and Consumer Act 2010 (Cth), the Australian Consumer Law (***ACL***)*

115. As set out in the Discussion Paper, the ACL applies to all products and services supplied to Australian consumers (except financial services), and this will include products and services that incorporate AI.[24]

116. Some of these basic rights include:[25]

a. consumer guarantees in relation to goods and services;
b. remedies depending on the level of failure in relation to meeting the consumer guarantees;
c. requirements in relation to the safety of consumer goods and services where the government can issue a mandatory safety ban where there is a risk of injury to a person; and
d. mandatory reporting for suppliers in relation to voluntary recalls and serious injury, illness or death associated with goods or services.

117. It is acknowledged by the ACL that loss or damage includes injury, per section 13 of the ACL.

118. We consider that the protections under the ACL could be broadened to include more applicable provisions to the use of AI, such as in relation to specific consumer guarantees for the provision of services where AI is being used to provide the service. Some of these guarantees could include guarantees that:

a. any legal or similarly significant decisions being made or contributed to by AI will be verified and monitored by a human; and
b. that any AI that is being used as part of the provision of services has been thoroughly tested for safety and accuracy and that any biases or limitations have been identified and reasonably mitigated.

119. A further requirement outside of the consumer guarantees that could be inserted into the ACL could be a requirement that any supplier of a service must disclose the use and role of AI in its provision of its services to consumers prior to consumers purchasing the service. However, these proposed changes could equally be placed in a new Australian AI Act.

22 *Ibid, p 9.*
23 *Ibid, p 9.*
24 *Australian Government, Department of Industry, Science and Resources, "Safe and responsible AI in Australia", Discussion Paper (June 2023), p 12.*
25 *Ibid, p 12.*

*Corporations Act 2001 (Cth) (***Corporations Act***)*

120. We consider that the Corporations Act may not be the best regulatory medium to address any regulations or requirements for private organisations in relation to the use of AI due to the current length and complexity of the legislation, and that the broad requirements for corporations under the Corporations Act are likely to already be applicable to the use of AI.

121. An example of a broad duty that is likely to capture the responsible use of AI by a company is the duty of care and diligence for directors and other officers under s 180(1) of the Corporations Act, which requires directors and other officers to exercise their powers and discharge their duties with the degree of care and diligence of a reasonable person. This duty has already been expanded to apply to a director's duty to ensure appropriate cyber security risk mitigation measures are in place for Australian Financial Services licensees.[26]

123. Another example is the duty of good faith for directors and other officers under s 181(1), which requires directors to act in good faith in the best interest of the company and for a proper purpose.

124. The requirement for responsible use of AI by Australian Financial Services Licensees (AFS Licensees) in their delivery of their financial services will also likely be captured by the broad arm of section 912A(1)(a) of the Corporations Act, which requires AFS Licensees to do all things necessary to ensure that the financial services the AFS Licensee offers are provided efficiently, honestly and fairly. For example, it could be argued that inappropriate use of AI could breach this general obligation where individuals are disadvantaged in their application for insurance cover due to an AI output caused by an algorithm that has been trained on incomplete or culturally skewed data.

*Copyright Act 1968 (Cth) (***Copyright Act***)*

124. While the code in computer programs is protected as a literary work under s 10(1) of the Copyright Act, we agree that the Discussion Paper has correctly identified the issues that AI presents in relation to how copyright law applies to text and data mining, database protection and the authorship of AI works.[27]

125. AI brings specific challenges to copyright law, particularly given that the rights of authors under copyright law generally vest in creation, and are not registrable rights. This makes the challenge of authorship difficult in particular.

126. We recommend that the Copyright Act is explicitly reviewed with recent technological developments in mind, including AI.

26 *ASIC v RI Advice Group Pty Ltd [2022] FCA 496.*
27 *Australian Government, Department of Industry, Science and Resources, "Safe and responsible AI in Australia", Discussion Paper (June 2023), p 36, Attachment A.*

*Online Safety Act 2021 (Cth)(***OS Act***)*

127. As set out in the Discussion Paper, the OS Act already includes mechanisms to address online safety issues that may involve AI, such as cyberbullying, image-based abuse (including deepfake pornography) and other kinds of material, as well as the powers for the eSafety Commissioner to require the removal of illegal and harmful content, including AI generated material.[28] The gap here is in relation to the use of AI in the provision of services to individuals where the issues anticipated by the OS Act are not always applicable.

128. We consider that addressing the responsible and appropriate use of AI in the provision of services, beyond online safety, is best addressed in other acts.

Fair Work Act 2009 (Cth)(**FW Act***)*

129. We consider that the FW Act may not be the most suitable regulatory medium to address any regulations or requirements for private organisations in relation to the use of AI due to the current length and complexity of the legislation, and that the broad requirements for entities and individuals under the FW Act are likely to already be applicable to the use of AI. For example, the prohibitions against discrimination are not limited in a way that would make it not applicable to AI systems.

*State/Territory based anti-discrimination legislation (i.e. the Equal Opportunity Act 2010 (Vic) (***EO Act***) in Victoria)*

130. Similar to the above, discrimination legislation may not be the most suitable regulatory medium to address any regulations or requirements for private organisations in relation to the use of AI due to the current length and complexity of the legislation, and that the broad requirements for entities and individuals under the legislation are likely to already be applicable to the use of AI. For example, the prohibitions against discrimination are not limited in a way that would make it not applicable to AI systems.

Common law of tort and contract

131. We consider that common law should be a last resort as a reliable mechanism for the Australian Government to rely on in relation to the responsible use of AI. This is because the enforcement of common law generally requires formal legal action, and the resources to take formal legal action are often not available to many individuals, unless the action is a class action.

Question 19

How might a risk-based approach apply to general purpose AI systems, such as large language models (LLMs) or multimodal foundation models (MFMs)?

132. Regarding general purpose AI systems, applying a risk-based approach could involve the following:

28 *Australian Government, Department of Industry, Science and Resources, "Safe and responsible AI in Australia", Discussion Paper (June 2023), p 10.*

a. Identification and classification of data or data sets used in training the model. Then providing a risk classification against this data and additionally the training process of the model.

b. Identification of the type of AI model used and assessing the risk impact of that AI model, identifying any proprietary or non-standard functional variations to the model which differs from standard risk classifications of said model type and have these variations independently assessed.

c. Performing a risk assessment relating to the output of the AI application, including implications and scenarios where the output data can be used by malicious parties or non-malicious parties with unintended malicious consequences.

d. Risk based assessment of developers and team involved in the development or consumption of the AI which can factor whether or not they have appropriate training or certification.

e. Implementation of appropriate controls which are validated by external experts and re-classification of residual risk.

Question 20

Should a risk-based approach for responsible AI be a voluntary or self-regulation tool or be mandated through regulation? And should it apply to: (a) public or private organisations or both? (b) developers or deployers or both?

133. Initially a risk-based approach for responsible AI should be voluntary or self-regulated with a view to eventually implementing a mandated regime for high-risk activities and organisation. This approach would apply to public and private organisations and developers and deployers alike. The issue with this approach is the increased likelihood of the generation of misinformation, cyber security threats and privacy threats to name a few. An issue which is creating a great deal of concern is the unregulated processing, storage and use of data for the creation of algorithms. This concern raises questions around the ethics of AI and how it is at the mercy of the data and/or instructions it is given.

134. Although Australia does not have specific legislation which contemplates AI it does have solid and broad technology laws which could be relied upon to govern AI activities in the interim. These fundamental laws along with specific AI guidelines provide a starting point for AI regulation and potentially allow for self-regulation currently.

135. Organisations such as KPMG are offering services by providing quality and risk managements frameworks for private enterprise. These services anticipate AI regulation and promote the benefits of being prepared for when AI specific laws are eventually implemented. Whilst Australia is taking a voluntary approach to AI regulation it would be prudent to make clear the regulation of AI is inevitable and organisations, developers and deployers should prepare accordingly. This may encourage the implementation of guidelines and principles for AI.

136. The benefits of risk based self-regulation is in creating guidelines or codes of conduct which are sector specific and have likely been overseen and applied by industry experts. Self- regulation models can also be quickly implemented and are often flexible and allow for innovation and development.

137. While self-regulation is at play the government has the option to mandate regulation for specific sectors and a risk-based approach would potentially highlight ongoing issues or identify issues which are high risk and may need to be subject to mandated regulation. A risk-based approach can also assess the impact of AI and where more structured and enforceable measures need to be taken or where a complete ban or moratorium is required. A voluntary risk-based approach has the ability to influence the public and private sectors and developers and deployers of AI by encouraging behaviour through the anticipation of regulation. This model also provides an agile environment which encourages innovation and inspires activities towards learning, embracing and harnessing AI.

Melbourne
Level 21, 114 William St,
Melbourne, VIC 3000
+61 3 9008 5954

Sydney
Level 11, 10 Carrington St,
Sydney, NSW 2000
+61 2 8315 3236

Brisbane
Level 8, 100 Creek St,
Brisbane, QLD 4000
+61 7 3123 6040

London
7 Pancras Square,
King's Cross, London, N1C 4AG
+44 20 4579 0889

LAW SQUARED

www.lawsquared.com