TELSTRA GROUP LIMITED

Safe and responsible AI in Australia

Public Submission

11 August 2023

Summary

Telstra welcomes the opportunity to provide feedback on the Department of Industry, Science and Resources discussion paper on Safe and Responsible AI in Australia.

Telstra is committed to the application of safe and responsible AI as demonstrated through our engagement with the Australian Government on the AI Ethics Framework and our work with the GSMA on the AI Ethics Playbook for the Mobile Industry. We have implemented a responsible AI policy within Telstra based on the AI Ethics Framework and we continue to develop practical tools that give our organisations guardrails for the safe and responsible design, development and deployment of AI.

AI has the potential to disrupt nearly every industry, promising both competitive advantage and creative destruction if not managed. The telecommunications sector is experiencing a significant and dynamic transformation. With the proliferation of smart phones, connected devices and the internet of things (IoT), the volume of data being generated and the opportunities and challenges that come with using it are front of mind for the sector, particularly given the high-profile breaches in recent years. In light of this, Telstra fully supports the development, by the Government, of a framework that both encourages and embraces innovation within an agreed set of boundaries that engenders community trust in the use of AI for all organisations. To this end we look forward to working closely with the Government and progressing safe and responsible AI in Australia.

Key Recommendations:

- We suggest leveraging the definitions for AI used in the ISO Standards to help align as much as possible with definitions used in international frameworks.
- We support an overarching AI governance framework, based on the current legal framework and supported by a range of other mechanisms including industry standards, guidelines and principles. The framework should focus on minimising harm whilst not limiting investment and innovation.
- We caution against the introduction of new AI specific legislation until a complete analysis of the existing mechanisms is undertaken to avoid the risk of duplication and increasing regulatory burden on industries.
- We recommend the establishment of one, nationally recognised body, similar to the Cyber Security Coordinator, to oversee the development and deployment of the AI governance framework, maintain visibility of activity both domestically and internationally, and report to government.
- We would encourage the Government to view data and AI as inextricably linked and in working through the potential gaps in regulation or otherwise consider also how data is being managed and aggregated.
- We advocate for close collaboration between the Government and industry to combat the rise in the use of AI for malicious purposes.

- We support the development of a framework which complements international regimes, but which also learns from those jurisdictions that have already implemented AI regulation or frameworks.
- In considering a risk-based approach we suggest the Government take a multidimensional view of risk to mitigate limitations. We recommend that the Government endorse a framework similar to that proposed by the GSMA, which can be aligned internationally.
- Transparency and contestability are essential for building trust in AI. Any proposed reforms should introduce definitions on automated decision-making and frameworks to contest automated decision-making.
- Defined roles and responsibilities help to provide oversight and accountability. We support these being established by individual organisations and not prescribed through regulation.
- We anticipate that the Government will play a crucial role in building confidence in AI particularly in relation to jobs and skills, and will need to use a multifaceted approach, such as through funding training programs, retraining initiatives, tax incentives for AI upskilling, encouraging the integration of AI-related topics into educational curricula, and awareness campaigns, to accomplish this.

Introduction

AI is an evolving technology that has the power to transform the way we connect and do business. It has enormous potential to drive efficiencies for both the gain of the Australian economy and individuals. We acknowledge the need to balance this enormous potential with the risks around data protection, identity and ethics. We believe that AI can be enhanced or limited by the data that feeds it. We see the potential for AI to redefine our customers' lives and livelihoods as well as how we do business, but that it needs to be trained in human centric and rights-oriented ways. As a leading player in Australia's telco and tech ecosystem, we have a role to play in the adoption, implementation and development of AI solutions. We believe that we should learn from jurisdictions that have already developed frameworks and regulations, as such we recommend Australia adopt frameworks which are similar to the GSMA AI Ethics playbook which is based on applying ethical principles within a strong governance structure and which was informed by EU regulation.

At Telstra we have developed a robust governance framework based on the Australian AI Ethics Framework. We have developed our own responsible AI policy and guidance documents, which incorporates our approach to risk assessment of new AI use cases. We believe this approach, that allows our organisation to take responsibility and accountability for the assessment of risk, provides for a better outcome for our own innovation but also the protection of our customers. As such, we support an Australian AI framework that safeguards the responsible use of AI in Australia that is outcomes focused rather than through prescriptive legislation.

We recommend that any AI governance framework focuses on enhancing the current regulatory framework (e.g. consumer protection, online safety, privacy and criminal regulation) so that it deals with liability and accountability for automated decision-making and responsibility where there is no human control or intervention. Any necessary legislative amendment should be technology agnostic so that the regulation continues to be relevant as the technology enhances and develops. The framework should also be supported by a range of other mechanisms including industry standards, guidelines and principles which encourage industry to manage their own risk to achieve a set standard that is focused on minimising harm whilst not limiting investment and innovation.

In our submission we discuss in more detail some of the issues that we see of great importance to developing a framework in Australia, followed by set answers to the specific questions asked by the Department of Industry Science and Resources. We note that, in some cases, we believe it is too early to develop substantial answers to some of the questions, in which case we have offered an initial view in response to such questions. We would welcome the opportunity to discuss our submission with DISR at the appropriate time.

Definitions

The definitions of AI that are adopted will be critical in the design of any regulatory frameworks and standards. These definitions will underpin every aspect of the governance framework, how it operates and what its reach is. Clear definitions will be critical to establish criteria and benchmarks for AI system safety, reliability, transparency, fairness, and accountability. However, because of the global nature of the technology, and the fact that many large Australian organisations have a global presence, or utilise technology from international vendors, it is essential that the definitions Australia

sets out to use are also aligned as much as possible with those used in international frameworks. We recommend this could be achieved by Australia leveraging the definitions used in the ISO Standards.

We note that Standards Australia has been engaged with the development of ISO standards on AI for several years, including definitions and terminology. We know that ISO develops and publishes standards through a rigorous and transparent process that involves the participation of experts, stakeholders, and industry representatives and that the standards are based on consensus, drawing on the collective expertise and experience of the participating members. Given this rigor we expect ISO standards will play a key role in unifying an approach to AI globally and we recognise they will set a benchmark. Adoption of ISO Standards will promote the development and advancement of best practices and standards within the AI industry locally and enable sectors that consume AI to manage their global supply chain risk through requiring adherence to ISO standards.

AI Governance Framework in Australia

We believe the current regulatory framework has the right fundamentals to address the risks created through the use of AI, and by enhancing this framework to deal with risks, liability and accountability introduced by AI systems, an AI governance framework can be created in Australia. If we consider the Privacy Act, there are already several obligations to protect personal information. These obligations are to be further enhanced as part of proposed reforms to the Privacy Act. Irrespective of the technology that may be ingesting data, the Privacy Act and Australian Privacy Principles apply to inputs and outputs that are Personal Information (PI) and as such, in the most part provide sufficient protection of PI irrespective of the technology that is processing the PI. Similarly, this same argument would apply to consumer protection laws through the *Telecommunications Act 1997* (Cth) which deals with the security and protection of telecommunications data and the *Australian Consumer Law* (ACL) which sets out basic rights for consumers when they purchase goods and services. This extends to marketing of products and services, safety standards, consumer guarantee's, product standards etc. The ACL imposes obligations on organisations in relation to misleading and deceptive behaviour and unconscionable conduct, all of which could be applied to the use and output of AI systems and the way that an organisation uses and makes decisions about a customer using AI or automated decision making (ADM).

However, the current legislation does not specifically address expectations in relation to the quality and completeness of the data being ingested into AI systems, which may result in biased or discriminatory outputs, and how AI systems are being trained culturally and ethically. Nor does it address copyright issues that may arise from the use of AI, or liability and protection for consumers where a machine has made an incorrect decision about an individual.

We believe that in order to address the gaps, the current legislative framework can be enhanced to deal with specific AI risks, further supported by introducing fluid and regularly reviewed standards and guardrails. We strongly caution against generating new AI specific legislation and regulation without, at a minimum, completing a thorough analysis of existing mechanisms. To introduce new AI specific legislation risks duplication and increases the regulatory burden on industries which could have a stifling effect on innovation. Further to this, it will make it difficult for the legal framework to stay abreast of the technological issues given the rate at which the technology is developing.

An AI framework should be supported by a range of mechanisms including industry standards, guidelines and principles which encourage industry to manage their unique risks to achieve a set standard that is focused on minimising harm whilst not limiting investment and innovation. Any changes to legislation or regulation should also be technology neutral so that they continue to be relevant as the technology evolves.

AI is evolving rapidly, whether in the context of the technology itself, or how it is deployed and used. While we acknowledge that this speed to market may inevitably open up gaps in existing regulation, as typically this is slower to respond and adapt, 'knee jerk' regulation creates unintended consequences and is not fit for purpose in the longer term. Robust non-regulatory arrangements can help bridge the gaps that long term regulation cannot, noting that any framework that is implemented will require a built-in, continuous cycle of consultation and review with industry, academia etc, and the ability to adapt and change to emerging developments.

Given the relative ease in which AI systems can be implemented, there is potential to underestimate not only the technological risks but also the reputational risks that unforeseen consequences may bring. In addition to the cycle of review any governance framework must also incorporate a component of guidance for AI adopters to upskill and be able to assess and avert potential brand and reputation risks.

Australia should adopt a nationally recognised AI body

Australia already has multiple government and non-government agencies and organisations considering the implications of AI. This approach creates the risk of disparate and potentially conflicting approaches being adopted. To support the cycle of review and adaptation that we believe will be required we suggest the Government consider establishing one nationally recognised body to undertake this important role, similar to the Cyber Security Coordinator, where cross field expertise can be brought together with a view to minimise harm and promote responsible and safe AI, within the existing regulation. This body could oversee the development and deployment of the AI governance framework, maintain visibility of activity both domestically and internationally, and report to government. The CSIRO has already made significant progress through their National AI Centre (NAIC) and their Responsible AI Network (RAIN), of bringing together experts, regulators, industry and academia. We suggest that extending the role and function the NAIC to be the AI Coordinator is a possible option.

Fundamentally an AI governance framework, must be established with a primary focus on protection rather than control. Specifically regarding the protection of people (individuals and groups) from AI related risks, rather than trying to prescriptively control the technology.

Data and AI must be considered together

AI is symbiotic with data. Data serves as the foundation upon which AI systems are built. It shapes the ability, accuracy, and performance of AI systems, while also influencing the potential impact on society. High-quality, diverse, and representative data is crucial to building ethical, unbiased, and effective AI solutions.

Good data hygiene is a considerable issue for any organisation to oversee and arguably it is the most important aspect to get right before AI capability can be realised. How an organisation aggregates, stores, and manages its data while simultaneously ensuring it is clean, accurate and error free will directly impact the application of AI. We appreciate that this consultation paper does not ask about or directly address data and its relationship to AI and we also acknowledge that the Government is progressing data security and value in other channels, we do consider the connection to AI to be important, and one in which should be acknowledged as part of any safe AI framework. Safe and responsible AI starts with the data that feeds it.

We encourage the Government to view data and AI as inextricably linked and in working through the potential gaps in regulation or otherwise, consider also how data is being managed and aggregated.

AI and Law Enforcement

To date, the development of foundational models that have accelerated AI visibility have been dominated by law-abiding organisations, there are, however, already reports of AI tools being used in the facilitation of criminal activity. The safe and responsible deployment of AI will extend beyond whether extra regulatory protections are needed for law-abiding organisations, it will necessitate close collaboration between the Government and the private sector to harness the power of the technology to also combat the potential for malicious development and usage of AI.

International Collaboration

Given Australia's desire's to be a global leader in the development of AI and our reliance on global supply chains to develop the technology, there are some practical and beneficial reasons for aligning to international regulatory frameworks. AI governance must be viewed through a global lens. AI cloud hosting, data sharing, co-design and joint research projects are already happening at a global level. By aligning our governance framework with trusted jurisdictions, we cannot only align and strengthen our protections but also maximise the opportunity for trade and innovation.

In order to build capability, we need to have uncomplicated trade avenues with our major partners. For example, the US and EU are already fostering a united, risk-based approach through the joint Trade and Technology Council, to bring their respective industries and governance frameworks closer together, to seize the opportunities but also mitigate the risks. We support greater international collaboration, and we would encourage the Government to utilise relevant multinational forums, such as the Global Partnership on Artificial Intelligence to look for opportunities that will bring us closer to our major partners.

Another example of the need for alignment is the fact that data can be stored, processed, accessed, and used offshore, and given the global digital market, Australian companies are already required to comply with international laws in relation to their data.

As such, we support the development of a framework which complements international regimes, but which also learns from those jurisdictions that have already implemented AI regulation or frameworks. We would also support the development of a set of technological international standards for AI technologies.

Risk-based Approaches

Telstra has adopted a risk-based approach to its assessment of AI use cases based on the GSMA AI Ethics Playbook and the Australian AI Ethics framework. At Telstra, when we use AI, our risk framework allows us to assess and test all stages of the AI lifecycle, this includes ensuring there is a clear purpose and set tasks, and that its performance is monitored, it understands our policies and procedures, and that it will protect our critical information. By applying our own internal risk framework applicable to the full AI development lifecycle we can ensure appropriate oversight and manage against risks so that they don't become systemic nor cause us to breach the law or negatively implicate our customers. As such we would recommend that the Government endorse a framework similar to that proposed by the GSMA, which has the ability to be aligned internationally.

We acknowledge that one limitation of risk-based approach's is that the different sectors across Australia's economy have varying levels of risk associated with the use of AI. For example using AI to make decisions about a patient's health care plan carries a very different risk profile to using AI to catalogue library books. Further to this, in some circumstances a risk assessment may return a high-risk outcome which could be acceptable under certain circumstances, but in others, such as the medical example, a high-risk outcome could be catastrophic. To address this issue, we recommend that all risk-based approaches need to adopt a reasonableness test to each assessment and require monitoring and oversight of all risk assessments. Industries should consider defining what constitutes high risk to avoid uncertainty and facilitate the application of appropriate controls in a consistent manner within a sector.

Governance should also not be contingent on maturity or resource strengths; it should always be appropriate for the risk. We recommend that part of an AI Coordinator's function should include educating and assisting organisations with limited maturity or experience in AI risk assessment and management to uplift their capability.

In considering a risk-based approach we suggest the Government take a multidimensional view of risk to mitigate some of the limitations outlined above.

Trust and Responsibility

To build and maintain trust in AI, we need to ensure the data being fed into AI systems has been assessed to minimise bias and discrimination. This includes using quality initial datasets, regular modal re-training, human oversight, not re-using datasets, and lifecycle management.

Building transparency and visibility into the AI lifecycle so that individuals understand how it is being used and is making decisions is an important element in building trust in AI systems but can also assist to improve accuracy and minimise bias and discrimination. Greater transparency in the way that AI is being used and developed can decrease the risk of error and misuse, enable internal and external oversight, distribute responsibility, and express respect for people[1], ultimately building trust. This should be coupled with the ability to challenge an AI decision or outcome that has a significant impact

[1] Building Transparency into AI Projects, Blackman & Ammanath, HBR, 2022, https://hbr.org/2022/06/building-transparency-into-ai-projects

to an individual. The current Privacy Act reforms[2] discuss automated decision-making, including providing meaningful information about legal or similarly significant decisions, but there is no specific proposal to enable contestability. Currently, this only exists as a voluntary guideline under Australia's AI Ethics Framework. Article 22 of the General Data Protection Regulation (GDPR) explicitly requires a right to human intervention and to contest a decision, but potentially only for 'solely automated decisions' that have a legal or similar effect or significantly affects a person. Any proposed legislative reforms should introduce definitions on automated decision-making and frameworks to contest those decisions.

AI model lifecycle must also be considered. Models drift and decay with time. When new, unseen data is introduced or the underlying assumptions about the data change, the reliability of the output could become impacted. Controls such as regular re-training, resetting and retirement should be built into the model lifecycle, particularly of high-risk use cases, along with regular audits of the effectiveness of such controls. Basic hygiene such as an inventory of data assets and AI systems, and a regular cadence of assessment on deployed AI models, should be used to ensure they are still performing within accuracy tolerance and that implemented controls mechanisms are, and continue to be, valid and effective.

Oversight and accountability are essential principles for AI policies and having clearly defined roles and responsibilities throughout the AI system lifecycle will help to build trust and confidence that AI systems are being managed responsibly. We emphasize the importance of mechanisms for oversight and accountability and recommend that they be established by individual organisations as part of a responsible AI framework. We would not support them being prescribed through regulation.

Workforce Upskilling

There is no doubt that AI is going to be a huge disruptor to the way we currently work. Most likely though, at least in the near term, it will not so much be a case of AI replacing humans but humans working with AI. The impact of AI is already reducing time consuming, repetitive tasks such as analysing large datasets, enabling people to focus on more strategic outcomes and complex human impact decision making.

The workforce will require upskilling in how to use AI effectively, particularly with regard to data literacy (how to work with data, draw insights from it and make data-driven decisions), and responsible use of AI, which will need to be reinforced regularly through compliance training. Smaller businesses will no doubt require assistance in this area, as they may not have the capability and/or resources to ensure they are using AI effectively and responsibly.

Both government and industry will need to work collaboratively to support an AI ready future workforce. Specifically the Government will play a critical role in helping to prepare through additional funding for training programs, retraining initiatives, tax incentives for AI upskilling, supporting the integration of AI-related topics into educational curricula, and general awareness campaigns.

[2] Attorney-General's Department Piracy Act Review – Discussion paper

Acknowledging that some Australians are hesitant about the impact that AI will have on jobs, greater visibility of government endorsement and support for the technology will also help build public confidence in a positive future.

Consultation Questions

Definitions	
1	**Do you agree with the definitions in this discussion paper? If not, what definitions do you prefer and why?**
	Clear definitions will be critical to establish criteria and benchmarks for AI system safety, reliability, transparency, fairness, and accountability. However, because of the global nature of the technology, it is essential that the definitions Australia sets out to use are also aligned as much as possible with those used in international frameworks. We recommend this could be achieved by Australia leveraging the definitions used in the ISO Standards. The definition of AI needs to take into consideration reforms to and existing limitations under other legislative frameworks. For example, the Privacy Act reforms include a new concept of 'targeting' where individuals will have the ability to opt-out of 'targeted advertising', so that their personal information cannot be used for tailoring services, content, information, advertisements or offers provided to or withheld from an individual. Given the definition of AI currently contemplates a system that generates content, forecasts, recommendations or decisions for a given set of human-defined objectives or parameters, it needs to be considered both in this context and the Privacy Act reforms if an individual opts-out of targeting, will that then mean that their information cannot be entered into an AI system at all to generate marketing insights. The definitions or any associated standards should also define what makes a decision fully automated, i.e. whether any human involvement is included in a fully automated decision and what is considered a 'high risk' use case, which is likely to be different for each sector. We would recommend that the definitions closely align with the OECD definitions along with consideration of the work on definitions being undertaken by the ISO. For example, the proposed definition of AI system under the EU AI Act is aligned with the OECD's definition of AI system, being "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." Inclusion of the word 'predictive' in the definition of AI restricts the scope of what may be considered AI and may be too limiting. In the event that the proposed definition is adopted, 'predictive' should be used as a noun to describe one type of possible output, rather than as an adjective to describe all types of outputs. For example, "AI refers to an engineered system that generates outputs such as content, forecasts, recommendations, predictions, or decisions…"
Potential gaps in approaches	

2	**What potential risks from AI are not covered by Australia's existing regulatory approaches? Do you have suggestions for possible regulatory action to mitigate these risks?**
	Australia's current regulatory frameworks whilst in the most part address general risks to individuals and their rights; and the obligations of corporations processing large volumes of data, there are areas that will not address specific risks created by AI and the use of automated decision-making. Examples of this include, risks associated with automated decisions based on data that is biased or discriminatory. Whilst the Privacy Act imposes obligations to ensure that data is accurate and up to date, it doesn't address discrimination or bias. We would recommend that bias and discrimination through the use of AI be addressed via federal anti-*discrimination laws such as, the Racial Discrimination Act 1975 (*Cth*), Sex Discrimination Act 1984 (Cth), Disability Discrimination Act 1992 (*Cth*), and Age Discrimination Act 2004 (*Cth*)* [3]. Our consumer protection legislation does not currently include processes to contest a decision that is a fully automated decision. Nor does it require an organisation to make it visible to an individual when a decision made about them is fully automated. For example, when an applicant for a job is rejected then it should be visible to them that the decision has come from an AI algorithm. Under the GDPR, Article 22 explicitly requires a right to human intervention and to contest a decision, but potentially only for 'solely automated decisions' that have a legal or similar effect. Consumer protection legislation will need to address how automated decisions can be contested and impose obligations on the public and private sector to make it visible if automated decision-making is being used in relation to decisions about an individual. The Corporations Act should address penalties associated with the generation of mass political or corporate misinformation generated by AI technology. Laws in relation to the use and protection of intellectual property will need to be reviewed to address how outputs from generative AI will not unintentionally breach another party's intellectual property rights to the source information. Where the intellectual property rights have been intentionally breached, the laws will need to address avenues for individuals to dispute such use. Issues such as who will be responsible and accountable for the breach will need to be closely considered. We recommend that the Government undertakes a holistic review of the existing legislative framework and identify the gaps (working with industry) that need to address specific AI risks, rather than introducing a separate AI Act. A separate legislative instrument, specific just to AI, runs the risk of introducing additional complexity that is not technology agnostic and therefore not able to evolve with the technology.

[3] page 46 HTI The State of AI Governance in Australia - 31 May 2023.pdf (uts.edu.au)

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.**
	Standards for supply of AI-based products should be introduced. This would allow Australian organisations to operate third-party products with more confidence. Like in the US, there are many not-for-profit (NFP) organisations and research-based organisations in Australia that are primarily working on building tools and capabilities which help measure safe and responsible use of AI by all organisations (Govt, NFP, FP orgs). These organisations should be provided funding to continue to improve, innovate and develop tools that can assist government and industry to implement organisational tools for the safe use of AI within an AI framework as we have discussed in our submission. But also should be coordinated to ensure a consistent approach to the development of such tools and capabilities.
4	**Do you have suggestions on coordination of AI governance across government? Please outline the goals that any coordination mechanisms could achieve and how they could influence the development and uptake of AI in Australia.**
	We recommend that Australia establishes or extends the role and function of a body like the NAIC or other group of experts to oversee the development and deployment of AI and maintain visibility of both domestic and international uses.
Responses suitable for Australia	
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?**
	We recognise the value in understanding and learning from governance measures adopted in other countries, however we should take from these approaches elements that are acceptable and workable for Australia and which are in line with our cultural expectations. Notwithstanding this, any measures we adopt need to allow for interoperability and sharing of data between other trading countries, such as the EU, US, UK, New Zealand and Canada. In Australia we need to manage the fine line between over-regulating to alleviate community concerns arising from the accelerating pace of AI developments against the risk of over-regulation stifling innovation and competition. As such, we support enhancing existing regulation which addresses key risks associated with the use of AI. We recommend that Australia adopts various measures that other countries are taking which are fostering the adoption and growth of AI that are workable for Australia and in line with our cultural expectations.

Target areas	
6	**Should different approaches apply to public and private sector use of AI technologies? If so, how should the approaches differ?**
	No. The framework should apply similarly across the public and private sectors. Applying different approaches introduces undue complexity and could impact collaboration and innovation between the public and private sectors.
7	**How can the Australian Government further support responsible AI practices in its own agencies?**
	The Australian Government needs to show how it is using AI and be transparent in relation to its risk management approach to the use of AI within government.
8	**In what circumstances are generic solutions to the risks of AI most valuable? And in what circumstances are technology-specific solutions better? Please provide some examples.**
	Risk-management solutions should focus on mitigating the impact generally rather than just applying to the technology where the problems first occurred. Technology-specific cases tend to exemplify the problem (e.g. failures in accuracy in facial recognition can lead to the potential for bias in a range of circumstances). Technology specific solutions are better for monitoring, ensuring compliance & controls and reporting. In most circumstances, human oversight and manual actions are important to manage risk (for example – fraud mitigation needs affirmation that a human is on the other side, not a robot).
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?** **(b) mandating transparency requirements across the private and public sectors, including how these requirements could be implemented.**
	(a) We suggest there are different requirements for transparency that span the development, operation and output of any AI system. Individuals need to be able to understand how an AI system is being used and making decisions about them. We believe that in all cases, transparency is essential. (b) In certain high-risk scenarios, where decisions or output could have a significant impact on individuals or groups, particularly where these are from fully automated systems, we support mandatory transparency and contestability requirements.

10	**Do you have suggestions for:** **(a) Whether any high-risk AI applications or technologies should be banned completely?** **(b) Criteria or requirements to identify AI applications or technologies that should be banned, and in which contexts?**
	(a) We recommend that high-risk AI applications are defined and that a process is introduced to assess any applications that fall within the definition. Similar to the process applied to the banning of inappropriate websites, high-risk AI applications should also be blacklisted. (b) As set out in response to (a) we agree that criteria should be developed based on a similar approach to the way malicious websites, viruses and bad actors are identified.
11	**What initiatives or government action can increase public trust in AI deployment to encourage more people to use AI?**
	We suggest the Government actively promote the activity they are undertaking to support the use of AI technology along with running education campaigns that engage with the school curriculum. Introducing a government endorsed 'AI Risk Assessment' document or process, that industry can align with will assist in building public trust in AI deployment.
Implications and infrastructure	
12	**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?**
	It could limit Australia's ability to innovate with AI, but equally it would align our approach with some of our trading partners, like the EU, and therefore it is unlikely to have limited downsides.
13	**What changes (if any) to Australian conformity infrastructure might be required to support assurance processes to mitigate against potential AI risks?**
	We believe that transparency and contestability process structures should be built into the AI lifecycle to support assurance to mitigation of AI risks.
Risk-based approaches	
14	**Do you support a risk-based approach for addressing potential AI risks? If not, is there a better approach?**

	We support a risk-based approach for addressing potential AI risks.
15	**What do you see as the main benefits or limitations of a risk-based approach? How can any limitations be overcome?**
	A risk-based approach to the adoption of AI allows businesses to innovate and develop AI solutions that align with a risk appetite acceptable to our society. It allows for an outcomes approach in comparison to prescriptive regulation which has the potential to stifle innovation and competition. The limitation is that there is then a tendency to create different solutions at different levels of risk rather than leveraging solutions that apply across all levels (e.g. selecting unbiased data sources would be good practice regardless of whether they are used in high or low risk scenarios). To overcome this, we should describe controls (e.g. any regulations) that are generic for any risk level but allow for a 'reasonableness' test in their application.
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?**
	It should apply across all sectors.
17	**What elements should be in a risk-based approach for addressing potential AI risks? Do you support the elements presented in Attachment C?**
	We support the elements presented in Attachment C.
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?**
	Please refer to our responses to questions 1 and 2.
19	**How might a risk-based approach apply to general purpose AI systems, such as large language models (LLMs) or multimodal foundation models (MFMs)?**
	We believe a risk-based approach works best when adverse events are understood. In this regard, risk management is retrospective after an adverse event. The challenge for general purpose AI systems is that today, we do not have clear line of site of the future specific uses these capabilities might provide. Therefore, future adverse events are difficult to predict. We believe a strong focus on ethical principles is one of a number of ways of reducing the likelihood of future adverse events from the use of AI. The Government should capitalise on Australia's

	progress and expertise in ethics to develop a strong framework that both Australia and the international community should operate within in relation to use and development of AI. We suggest the Government consider establishing one nationally recognised body to oversee the development of AI in Australia.
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?**
	We believe it is too early to comment in relation to this and that we should re-assess the effectiveness of global legislation in 3-6 months as we develop our own framework.