Supporting responsible AI: discussion paper

Make a submission

Department of Industry, Science and Resources

Response received at:
26 July 2023, 6:00am

Response ID:
sbm2826e0fc81e471c397e3e

1 Do you agree to the Privacy Collection Statement?

Yes I agree

2 Please indicate how and if you want your submission published.

Public

3 Published name

IoT Alliance Australia

4 First name

Frank

5 Last name

Zeichner

6 Email

frank.zeichner@iot.org.au

7 Phone

0408233762

8 Who are you answering on behalf of?

Organisation

9 Organisation

IoT Alliance Australia

10 What sector best describes you or your organisation?

Peak or professional body

11 What state or territory do you live or work in?

New South Wales

12 Postcode

2000

13 What area best describes where you live or work?

City

14 Have you removed any identifying information from your submission?

Not answered

15 Upload 1

IoT Alliance Australia submission - Safe and responsible AI in Australia - 26 July 2023 - Final.7ee2f82426725.docx

16 Upload 2

Not answered

17 Upload 1

Not answered

18 Upload 2

Not answered

19 Make a general comment

Internet of Things Alliance Australia (IoTAA) thanks the Department of Industry, Science

and Resources for the opportunity to submit feedback to the Safe and responsible AI in Australia consultation.
IoTAA is the peak body for the Internet of Things (IoT) in Australia. A non-profit industry association, IoTAA was formed in 2016 to enable a data smart Australia, which advances society through trusted, accessible real-time data, powered by Internet of Things technologies. AI technologies are an integral part of the IoT technology suite, whether at the collection point in sensors, at the edge or in the core network for centralised intelligence – and at many points in the data chain across multiple entities.

20 Do you agree with the definitions in this discussion paper? If not, what definitions do you prefer and why?

Yes. The definitions on page 5 are based on international standards which a solid starting point.
The distinction between AI and ML is an important one. AI generally involves coded algorithms which involve human design. As a consequence, they:
- Can be explained in human terms.
- Can be made visible and transparent.
- Can be inadvertently biased.

Machine learning (ML) are patterns that are recognised from training data. These patterns are not human designed and may not be readily explained by humans in their operation or effect.

21 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?

Mitigating risks of AI requires attention to be placed on:
- Responsible training for providers and users
- Responsible deployment – where and with whom AI is applied
- Transparency
- Appropriate controls

The risks from AI that may not be covered in existing regulatory approaches, would seem to generally arise from:
- Lack of transparency and understanding of how decisions are made. The problem here being the inability to access how the AI is applied, often because of commercial reasons.
o Note, ML may pose a greater risk as it's decision making is less programmed and deterministic.
o Lack of transparency will also mask underlying issues such as intended or unintended bias. This may have significant social and pollical impact in the case of manipulative uses

of AI
Transparency and disclosure requirements might be applied economy-wide to commercial
offerings of an AI product or service that is intended for use by a customer, whether a business customer or a consumer.

These requirements could take the form of new provisions in Australian Consumer Law and
analogous requirements in sector specific laws, such as the Corporations Act, that ensure economy wide coverage of such provisions. AI products and services create issues as to gaps in coverage of Australian Consumer Law, and in particular operation of the definitions of “consumer”, “goods” and “services” as used in the ACL, and the consumer guarantees under the ACL.

Many of these issues of gaps in coverage, and similar issues as to appropriate allocation as between providers and customers of responsibility and accountability to anticipate, assess
and mitigate risks of harms, also arise in relation to deployment of internet of things consumer (“smart’) devices and IoT device enabled internet connected (‘smart’) services.

AI adds further categories of risks of harms to those arising from smart devices
and services. We commend consideration of applicability to AI systems of the recommendations and analysis of Professor David Lindsay, Genevieve Wilkinson and Evana Wright (each of UTS Sydney) as to how the Australian Consumer Law should be adapted to facilitate safe and responsible adoption in Australia of smart devices and smart services

22 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.

There are a host of initiatives the Australian government and its agencies could implement to improve AI-affected decision. These include:

- information and educational resources: improving competencies of people within organisations, and of other stakeholders (including industry associations, consumer organisations and civil society organisations), in AI-affected decision problem definition: that is, improving their competency to foresee a risk of harms to humans or environment that is reasonably attributable to a proposed use of AI,
- processes for gating of AI and evaluation of AI: frameworks (including standards),

methodologies, tools, checklists to assist myriad organisations to better assure adoption of a considered approach in determining whether, when and how AI is used, for which use cases,

- governance of AI-affected decisions within organisations: who considers what, in consultation with whom, before use of AI,
- safeguards and associated assurance (reliability and verifiability) controls, including ensuring post-implementation monitoring and reassessment based upon results and outcomes,
- allocations of responsibility and accountability within organisations for AI-affected decisions: identification of main individual actors and sub-units who are accountable, focussed upon the outcome or result of a decision chain that includes an AI link in the decision chain, and not just the output from the AI link in the decision chain

23 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.

As well as canvassing proposals for new AI regulation, the Australian government should promote discussion as to how Australian federal, state and territory governments, through
initiatives of government agencies and regulators, can effectively influence decisions by regulated entities, including other government agencies, businesses and not-for-profits, as
to whether, when and how to safely and responsibly use AI.

There are a number of developing international models of regulation of AI. For example: an
interventionist and prescriptive proposed in the EU AI Act , the draft Canadian AI and Data Act or the UK's proposed lighter touch, coordinated and decentralised approach .

We lean towards UK Government approach which proposes creation of central functions to support the multi-regulator, decentralised frameworks, including by:

- developing a central monitoring, evaluation and risk assessment framework,
- creating a central guidance to businesses looking to navigate the AI regulatory landscape in the United Kingdom,
- offering a multi-regulator AI sandbox, and
- supporting cross-border coordination with other countries.

24 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?

Please see our response to question 4

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

Approaches to the public use of AI should in general be held to a higher standard that for private use. As government use of AI for public use is often accompanied by compelling incentives, this should be matched with a higher level of compelling accountability and responsibility.

26 How can the Australian Government further support responsible AI practices in its own agencies?

Please see our responses to questions 2 and 3.

27 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.

Regulation should focus upon ensuring that organisations design and implement policies and programs for responsible uses of AI that are appropriate to the organisation and not the manner in which those policies and programs are implemented.

Generic solutions will be of most value and should incorporate the key externalities to determine whether services using AI are risky or not: that is vital externalities such as the quality of the data, the outcomes achieved and the people using the results. These would/should also be based on persistent ethical and social capital principles – as well as law.

Technology specific solutions are less effective and will require constant updating and revision, as new innovations and inventions appear. The result will undoubtedly lag effect.

Having said that, some specific technology solutions would include;

- Providing transparency and disclosure of algorithms for high-risk applications
- Considering adaptation of Australian Consumer Law to facilitate safe and responsible adoption in Australia of smart devices and smart services . See our response to question 1

28 Given the importance of transparency across the AI lifecycle, please share your thoughts on:

“Frontier” AI that is new and unproven AI is especially risky, given it’s unproven and untested effect. The attached paper considers options for broadening risk assessments to accommodate these risks – with a focus on extreme risks.
A good approach to AI regulation is to ask whether rules that restrict or prohibit particular uses of AI, or that mandate application of a particular risk assessment framework
or methodology, are justified, or whether ‘detect’ and ‘respond’ incentives as adjusted for AI would then provide sufficient incentives to cause appropriate mitigation of AI risks by regulated entities.

In the absence of sufficient detect and respond incentives, for specified AI-affected activities that are reasonably likely to lead to significant harms to some humans or the environment, then AI regulation, in the form of before-the-event prohibitions or prescriptions or both, may be justified. In that case, it is still appropriate to ask whether these risks of harms are:
- short-term and transitional - likely to be addressed through other government and industry initiatives to improve understanding as to responsible AI practices, or
- longer term or more entrenched and therefore requiring more intrusive regulation.

29 Do you have suggestions for:

There are applications that might be considered for banning – e.g. those that break the law, cause harm etc. These are likely mostly covered by existing laws.
b. Criteria or requirements to identify AI applications or technologies that should be banned, and in which contexts?
High risk AI that should considered to be managed, or even banned in special instances, are those where the lack of transparency and/or governance renders its effect opaque to users and may therefore mislead, be biased, discriminate etc. – if used in high risk use cases e.g. medical decisions with potential harmful outcomes
A category of AI which would fall into the high risk category is manipulative uses of AI. These may be not obvious in effect at first and difficult to assess. This category would tend to apply more to very broadly available uses of AI.

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

Please see our responses to question 3

31 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?

No comment

32 What changes (if any) to Australian conformity infrastructure might be required to support assurance processes to mitigate against potential AI risks?

No comment

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

Yes, a risk-based approach is the best way to address risks of AI harms. Each AI-enabled, or AI-assisted, decision requires consideration of decision provenance: the interaction of input data, people, processes, outcomes and technologies that affect that decision. There is no best one-size-fits-all approach to risk assessment and management, however any risk assessment should include at the above important aspects:
o of the AI technology itself – e.g. is it well designed, tested, free from obvious bias, clear in its purpose, transparent to users
o the application and effect to which the AI is applied – e.g. are the decisions to be made by the AI in a high risk context – e.g. life and death decisions for health
o to what degree do the people involved in providing the service and using the using need to know about how the AI works
o is the data input provided accurate?

We advocate policies and programs focussed on enforced self-regulation as the cornerstone. Assurance of safe and responsible uses of AI needs to become part of the DNA of each organisation - public and private, business and not-for-profit, large and small - and
consistently and reliably applied in the course of each organisation's business-as-usual processes. We do not support a prescriptive specification of how AI risk assessments should be undertaken, or the form that they should take.

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

Most organisations operating in Australia that are implementing AI within the organisation
will not be developers and suppliers of AI solutions. Typically, an organisation operating in Australia will be tailoring a third-party AI application or service and using it:

- more commonly, to inform or otherwise aid people within an organisation to perform a decision -making task, or
- much less commonly, to enable a fully automated (self-actuating) outcome

Senior executives and managers within organisations may not see a business process (decision chain) within the organisation as an 'application of AI', or even as significantly affected by AI.

Supporting programs suggested in our response to question 3 are vital in helping address these limitations.

Organisations could be required to develop and implement policies and programs to act responsibly and ensure safety in organisational uses of AI. As a minimum, organisations should be required to prepare an annual plan setting out what they propose to do about ensuring safety in organisational uses of AI, including specification of reasonable precautions that the organisation is putting in place.

This mandate could be supported by mandated transparency requirements, i.e., to publish risk of AI harms policies, and overviews of risk of AI harms programs.
There would need to be associated meaningful legal exposures for organisations, and their
directors and their senior officers, in the event that the organisation:
- did not develop and oversee reliable implementation and operation of policies and programs,
- did not take reasonable precautions to mitigate reasonable foreseeable risks of AI harms, or
- did not comply with transparency requirements.

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

Those sectors who already have established or are establishing risk-based assessment and associated governance, such as those service providers of critical infrastructure, would be better placed to accommodate additional risk parameters around AI.

Many/ most organisations are not large businesses that have experience, settled procedures,
internal capabilities and resources to reliably evaluate a third-party AI application or service

for fitness for purpose for reliance in a particular business context, and assess the quality of
data inputs used by the AI provider to train that AI.

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

The elements summarised in Attachment C are relevant but incomplete, partly because the focus in Attachment C is upon assessment of the AI system itself, rather than the decision context that is being affected by the AI.

The risk based approach should be simple enough to enable everyday use of AI for low risk applications, for which there are a huge number of instances to be easily identified, and proceeded with, without further government intervention.

We disagree with the apparent presumption in Attachment C that all impact assessments should be published, or that "peer review" of impact assessments "by external experts" would significantly reduce risks of AI harms.

37 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 see our response to question 14.

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

Many Australian organisations that do not have capabilities to implement complex structured risk management frameworks or methodologies will be implementing generative
AI to assist non-technical humans to perform myriad tasks.

A risk management approach, coupled with an enforced self-regulation model, should be applied to general purpose AI services, designed to address the challenges associated with:
- lack of organisational control over how it is likely to be introduced into and used in many organisations for a myriad of tasks,

- the role of individuals within those organisations in determining when and how general purpose AI services are used as a task assistant, and the best ways to ensure those individuals exercise appropriate restraint and care,
- the key role that transparency can play in building awareness of risks and capability to mitigate risks.

For AI of extreme risk in frontier applications, a more rigorous risk assessment approach will likely be required.

39 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 risk-based approach for responsible AI should be applied by:
- both developers and deployers of both foundational models and algorithmic decision-making systems and generative AI applications built upon those foundational models or algorithms, and
- organisations, both public or private, that are users of third party supplied foundational models, algorithmic systems, at least to determine whether risks of AI harms are sufficiently likely to have been assessed and mitigated by upstream developers and providers