Commonwealth Bank

# Safe and responsible AI

*Response to Discussion Paper*

August 2023

Public

# 1. Executive Summary

The Commonwealth Bank of Australia (CBA) welcomes the opportunity to respond to the Australian Government's Discussion Paper – *'Safe and responsible AI in Australia'* (Discussion Paper).

CBA supports the Discussion Paper's consideration of regulatory and governance measures to mitigate the potential risks from Artificial Intelligence (AI) and to increase public trust and confidence in AI's development and use.

The Government's consultation is both timely and important. A recent study published by the University of Queensland and KPMG concluded that 71 per cent of people expect AI to be regulated, and that 61 per cent of people believe the long-term impact of AI on society is uncertain and unpredictable.[1] Close to one third of people lack confidence in government and commercial organisations to develop, use and regulate AI. This suggests that demystifying AI, optimising regulatory frameworks, and clearly communicating how regulation mitigates risks should be a priority for government and industry alike.

CBA's investment in AI has been a core strategic focus for a number of years. We were among a small cohort of companies that worked with the Australian Government to participate in the Australian AI Ethics Principles pilot that aimed to demonstrate how AI can be deployed safely, securely, and reliably.[2] We have developed training modules with Australia's leading research institutions to build the capability of our people working with AI.

We currently use AI to deliver more personalised services and seamless experiences for our customers and employees. We also use it to help keep our customers' money and data safe, which includes improved detection of fraud, scams and cyber threats, as well as tackling abuse in transaction descriptions. As we expand the use of AI to applications across our organisation, CBA remains committed to ensuring our use of AI is underpinned by fairness, transparency, privacy and security, reliability and safety, accountability, and human, social and environmental well-being.

In this submission, we outline CBA's views on a number of issues raised in the Discussion Paper. In summary:

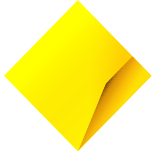
- CBA supports a technology neutral, principles led, and risk-based approach to regulation governing AI technologies, with greater guidance and coordination from government as to how organisations using AI technologies can conform to existing laws and regulations that govern data protection, privacy, consumer protection, discrimination, competition, and corporations across industries, as well as relevant sector-specific regulations.
- This is not to say that regulatory enhancements won't be needed as the risks posed by AI are real and complex, and will continue to evolve. CBA is of the view that the vast majority of risks associated with AI are extensions of existing risks that are already regulated under existing frameworks, and that therefore, AI-specific laws should be the exception. It is important to recognise the use of computer algorithms to analyse data has been around for many years and have been effectively governed, along with organisations (including CBA) establishing internal policies and processes around these models.
- In a few limited cases, there may be specific circumstances in which bans on AI may be appropriate where the risk is not appropriately dealt with by existing law. The Government should consult further on appropriate regulatory responses to high-risk AI applications.

---

[1] 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. https://ai.uq.edu.au/files/6161/Trust%20in%20AI%20Global%20Report_WEB.pdf, page 4

[2] https://www.industry.gov.au/publications/australias-artificial-intelligence-ethics-framework/testing-ai-ethics-principles/ai-ethics-case-study-commonwealth-bank-australia





- AI regulation should seek a balance between technological development and appropriate consumer protections.
- CBA believes a risk-based approach, as set out in the Discussion Paper, is well suited to both public and private sectors, and that risk-based approaches provide the most adaptable approach to address AI-related risks that will continue to emerge as AI technologies develop.
  Noting the global nature of AI development and the inconsistencies of AI regulatory frameworks emerging internationally, it is critical that Australia's AI regulatory environment remains interoperable with international frameworks. Australia should continue to lead on the development of international standards.

# 2. Defining AI

CBA believes governments and regulators should continue to leverage widely held definitions rather than establish new ones. As noted in the Discussion Paper, the International Organization for Standardization (ISO) states that AI is an engineered system that generates predictive outputs such as content, forecasts, recommendations or decisions for a given set of human-defined objectives or parameters without explicit programming. CBA supports this broad definition of AI that may include any products or services using AI techniques, and that these techniques may range from simple rules-based algorithms guided by human-defined parameters to more advanced applications.

Consistent with our view that AI-specific laws and regulations are not needed; we believe a prescriptive AI definition is unnecessary and could embed rigidity into the AI regulatory framework and become outdated and restrictive as AI technologies continue to evolve. We note this approach has been favoured by the United Kingdom (UK) Government in their recent 'pro-innovation approach' towards regulating AI.[3]

# 3. Gaps in approaches

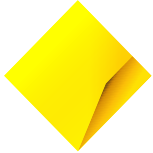
Given the rapidly evolving nature of AI, both in terms of the increase in use cases and increased access by consumers and businesses; there are likely to be gaps in Australia's regulatory framework for which guidance, interpretation and judgement is required. This is particularly the case with regard to the Generative AI that will challenge traditional intellectual property laws.[4] Enhancements to Australia's regulatory frameworks governing AI is therefore both inevitable and desirable.

In banking and financial services, mitigating AI risks are already covered under various laws and regulations, such as a licensee's obligation to provide services 'efficiently, honestly and fairly' under the *Corporations Act 2001*, consumer and competition laws, duty of care, Design and Distribution Obligations, the *Privacy Act 1988*, Banking Code of Practice, and prudential regulation for those entities regulated by the Australian Prudential Regulation Authority (APRA). In addition, there are industry standards that help inform the core regulatory obligations mentioned above, such as Australia's AI Ethics Framework.

Despite our belief that existing laws are, at least in the context of financial services, appropriate for managing the risks associated with AI, we recognise there are areas of legal uncertainty in relation to intellectual property in an AI context. Examples include: what level of human input is required in order for works generated by AI to be protected by copyright; and who bears responsibility in the event that AI outputs infringe third party intellectual property. We anticipate that more clarity will emerge as litigation in this area increases and the courts have the opportunity to consider these issues. Amendments to the

[3] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1146542/a_pro-innovation_approach_to_AI_regulation.pdf, page 22
[4] https://www.ipaustralia.gov.au/news-and-community/news/2023/07/07/04/48/generative-ai-and-the-ip-system-what-does-it-all-mean#:~:text=Generative%20AI%20will%20mean%20more,and%20how%20it%20is%20administered





*Copyright Act 1968* are also an option for addressing these areas of uncertainty, which could be explored as part of the Federal Government's ongoing Copyright Enforcement Review.

It is clear that there are indications that Australians believe that new regulation is required, with a University of Queensland survey finding that only two in five people believe current regulations, laws and safeguards are sufficient to make AI use safe.[5] However, these surveys are based on impressions and without any context about what regulation may exist in a particular sector. We believe that if informed about the existing laws that apply in a financial services context, the survey results may change and there is no need for additional legislation as it already exists to ensure the safe and fair use of AI in the sector.

CBA believes there are a number of initiatives that can be taken in the short term to enhance the approach across the economy in connection with the use of AI. The following initiatives should be considered to optimise and supplement the existing regulatory framework to support responsible AI practices in Australia:

### *a) Enhanced coordination mechanism for current AI regulatory frameworks*

CBA believes there is merit in initiatives that aim to enhance central coordination of regulatory issues affecting AI. This has been a focus of the current UK inquiry into AI regulation.[6]

Practical initiatives proposed in the UK focus on enhanced monitoring, assessment, and feedback on how AI is interacting with the regulatory environment. These include:

- Development of a central monitoring and evaluation framework to assess cross-economy and sector-specific impacts of the new regime;
- Ensuring appropriate data is gathered from relevant sources – for example, from industry, regulators, government and civil society – and considered as part of the overall assessment of the effectiveness of the framework; and
- Support to equip regulators to undertake internal monitoring and evaluations, and monitoring the regime's overall effectiveness.

There have been recent calls in Australia for centralised entities to aid in the coordination of Australia's existing AI regulatory framework. This was a key feature of the Australian Human Rights Commission's recommendation for the creation of an AI Safety Commissioner to support regulators, policy makers, government, and business in applying laws and other standards relevant to AI. As per recommendation 22 of AHRC's 2021 'Human Rights and Technology Final Report', an AI Safety Commissioner should:

- work with regulators to build their technical capacity regarding the development and use of AI in areas for which those regulators have responsibility;
- monitor and investigate developments and trends in the use of AI, especially in areas of particular human rights risk;
- provide independent expertise relating to AI and human rights for Australian policy makers; and
- issue guidance to government and the private sector on how to comply with laws and ethical requirements in the use of AI.[7]

CBA would welcome the expansion of the remit of an existing government agency to make it clear that it is responsible for the coordination of AI regulatory issues. There are parallels to be drawn from recent developments in cyber security, where the National Cyber Security Coordinator has been appointed to

[5] https://ai.uq.edu.au/files/6161/Trust%20in%20AI%20Global%20Report_WEB.pdf. Page 4
[6] https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper
[7] https://tech.humanrights.gov.au/artificial-intelligence/ai-safety-commissioner#:~:text=The%20Report%20recommends%20the%20creation,for%20AI%2Dinformed%20decision%20making.



coordinate a whole-of-government approach on cyber security policy and with government partners to ensure alignment across regulatory and incident response frameworks.[8]

While CBA would support the expansion of the existing remit of a government agency to champion AI, build trust, and coordinate regulation, the function would need to work closely with, and not duplicate, roles performed by the Australian Information Commissioner, National Data Commissioner, Chief Scientist, and National Cyber Security Coordinator.

*b) Support for regulatory sandbox initiatives to build AI capability and horizon scanning*

CBA shares the Government's desire to grow Australia's domestic AI industry by building capability and innovation in AI. Regulatory sandboxes can help industry navigate regulatory frameworks and give regulators a sense of what new technologies are on the horizon, which may require guidance, or in some case, regulatory reform.

Regulatory sandboxes allow for testing of innovative AI products in the real-world under relaxed regulatory requirements, but with appropriate safeguards in place on a time-limited and small-scale basis. Depending on the experiment, the sandbox may provide appropriate regulatory support by temporarily easing certain regulatory requirements for the duration and space of the sandbox.

CBA encourages support for AI-focused regulatory sandboxes noting that such initiatives are proposed in the European Union (EU)[9] and the UK[10]. In the EU, privacy regulators use regulatory sandboxes to great effect, allowing organisations to receive detailed guidance from regulators to implement 'privacy by design' systems, which CBA would welcome in the context of AI models. Specifically in financial services, regulatory sandboxes have been established in Singapore[11] and in Australia by ASIC's Enhanced Regulatory Sandbox, which was updated in 2020.[12] CBA would welcome the expansion of ASIC's sandbox to cover AI test cases and be made available to all financial market participants to encourage further innovation and collaboration between both existing participants and new market entrants.

*c) Development of the capability and methodology of properly assessing the risks of AI*

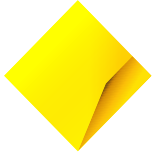
Any regulatory response must look to mitigate the risks that AI presents to consumers, businesses and the community as a whole. To assess the appropriate response, Government should continue to build the capability to understand the risk profile of AI and as it continues to develop, understand how these risks are changing. This risk assessment should be published on a regular basis and directly inform regulatory change and updated guidance on the applicability of existing laws. This should create mechanisms to leverage industry and academic expertise to ensure different perspectives are considered.

Once this risk assessment is finalised, in considering whether regulatory change is necessary, it is important that policy makers focus on the intended outcome of existing laws and whether that outcome is compromised as a result of the development of AI. For example, the prohibition of misleading and deceptive conduct is not restricted to how the conduct is developed. If the conduct is influenced by AI and is misleading and deceptive, the prohibition would still apply in the same way as it would apply to conduct that did not involve the use of AI.

In undertaking the risk analysis, it is likely to become clear that some risks cannot be mitigated through increasing the regulatory burden on companies that legally operate in Australia. Some risks will be created

[8] https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/cyber-coordinator
[9] https://www.eipa.eu/publications/briefing/sandboxes-for-responsible-artificial-intelligence/
[10] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1146542/a_pro-innovation_approach_to_AI_regulation.pdf
[11] https://www.smartnation.gov.sg/initiatives/business/fintech/
[12] https://asic.gov.au/for-business/innovation-hub/enhanced-regulatory-sandbox/info-248-enhanced-regulatory-sandbox/





by entities operating overseas that do not intend to comply with Australian law and do not have any assets in Australia. The use of AI in the context of scams is a good example of where, in many instances, the criminal activity is being undertaken outside of Australia by individuals and organisations that do not comply with Australian law. Therefore, restricting the use of AI in Australia to try and manage this risk will have very little impact.

*d) Restrictions on the use of sensitive information to test bias in AI models*

One of the specific gaps CBA has observed is the restrictions placed on the collection and use of sensitive information, including consent requirements, under the Privacy Act. These requirements become problematic when companies want to use sensitive information to conduct bias assessments to ensure AI models are operating as intended and free from negative biases.

Currently, the EU has proposed the introduction of a number of safeguards for the process of conducting bias assessments that would facilitate the use of sensitive information for these purposes. For the processing of such sensitive information, the bias must not be detectable by processing synthetic, anonymised, pseudonymised or encrypted data. The assessment must also happen in a controlled environment and the sensitive data cannot be transmitted to other parties and must be deleted following the bias assessment. CBA would support a similar approach being adopted in Australia.

# 4. International developments

Regulating AI remains a dynamic space internationally with different regimes emerging in various jurisdictions, both in terms of their intent and approach to regulating AI. There has historically been a lack of global consensus or cooperation on Ai though G7 digital ministers recently agreed that their countries should adopt risk-based regulation on AI, strive for interoperability across AI governance frameworks and support the creation of technical standards for implementation.[13]

The National Innovation and Science Council's (NISC) Rapid Response Information Report on Generative AI traces recent developments in the global effort to regulate AI.

We have outlined below developments in the EU, UK, and US to demonstrate different approaches and suggest how Australia should respond. Ultimately, CBA believes the uncertainty of AI regulation around the world adds weight to Australia maintaining a principles led approach, leveraging our existing framework and regulators, and not rushing to introduce prescriptive Australian laws and regulations. Additionally, there is a need for Australia's regulatory framework on AI to remain interoperable with other international regimes.

*a) European Union*

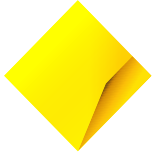
As noted by the NISC, the EU model is notable for differentiating between AI use cases: banning unacceptable uses and identifying others as 'high risk', where active ex ante compliance and ongoing monitoring is required. The model applies differentiated obligations on actors within the AI supply chain: providers, suppliers, importers and users.[14]

Although the European Parliament recently approved the draft EU AI Act, it is likely to take years to come into force in amended form after further negotiation with the Council of Europe and the European

[13] Ministerial Declaration The G7 Digital and Tech Ministers' Meeting (30 April 2023) - http://www.g7.utoronto.ca/ict/2023-declaration.html

[14] https://www.chiefscientist.gov.au/sites/default/files/2023-06/Rapid%20Response%20Information%20Report%20-%20Generative%20AI%20v1_1.pdf, page 15





Commission. Still, the EU regime warrants close attention. If and when the EU Act comes into force it will impact organisations operating outside the EU through at least three channels:

- market access, as non-EU organisations will have to comply with EU rules to access the common market;
- standardisation, as the EU Act will rely on yet-to-be-determined harmonised standards for much of its compliance, which are likely to incorporate or mirror international standards currently under development; and
- regulatory cooperation, as the Act will encourage the EU's trading partners to coordinate and align on interoperable AI rules, including via multilateral and bilateral agreements.[15]

The evolution of Australia's regulatory framework will have to factor in, and align to, international approaches given the global nature of AI, and the extra-territorial application of laws, especially from the EU.

### *b) United Kingdom*

As previously noted, the UK Government recently released its approach to AI regulation. The key components of the UK approach involve its reliance on existing legal frameworks, rather than implementing new AI-centred legislation; applying five general principles to be applied by regulators in conjunction with existing laws; and allowing regulators to adapt the five principles to regulated entities, with support from a central coordinating body. The five principles are as follows:

- safety, security and robustness;
- appropriate transparency and explainability;
- fairness;
- accountability and governance; and
- contestability and redress.

Advocates for the UK framework highlight it is designed so rules can be easily tailored and adapted much faster than the model emerging in the EU. A sector-based approach allows flexibility for existing regulators to address and manage the impact of the use of AI in their sector, including in response to new technological developments and specific AI use-cases, applying their contextual expertise to consider any gaps in existing sector frameworks and impose the appropriate level of scrutiny.

By leveraging a sector-based approach, UK regulators will be empowered to address risks as they arise and bypass lengthy debates in parliament should laws need to change. This is important given the velocity of AI development.

CBA favours a sector-led approach to AI regulation similar to that proposed in the UK. However, in recognising that Australia will be a net importer of AI technologies for some time, it is important for Australian policy makers to have regard to key international developments, such as the EU, and foster alignment where appropriate.

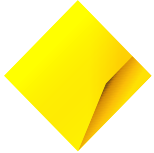
### *c) United States*

To date, there has been no serious consideration of a US analogue to the EU AI Act or any comprehensive federal or state legislation to govern the use of AI. However, there have been recent developments to signify critical steps in the US to manage the risks posed by AI.

---

[15] Human Technology Institite (University of Technology Sydney, the State of AI Governance in Australia) - https://www.uts.edu.au/sites/default/files/article/downloads/HTI%20The%20State%20of%20AI%20Governance%20in%20Australia%20-%2031%20May%202023.pdf





On 21 July 2023, the White House announced seven leading AI companies had agreed to voluntary safeguards, pledging to manage the risks of new AI-tools, and help move toward safe, secure, and transparent development of AI technology.[16] Some of the commitments made include the following:

- internal and external security testing of their AI systems before their release;
- sharing information across the industry and with governments, civil society, and academia on managing AI risks;
- facilitating third-party discovery and reporting of vulnerabilities in their AI systems;
- publicly reporting their AI systems' capabilities, limitations, and areas of appropriate and inappropriate use; and
- developing robust technical mechanisms to ensure that users know when content is AI generated, such as a watermarking system.

The White House announced that it is currently developing an executive order and will pursue bipartisan legislation to help America lead the way in responsible innovation. While US regulatory frameworks focused on AI may not be as advanced as those pursued in the EU or UK, it is important that Australian policy makers monitor developments in the US given the leadership role that the US plays in AI technology development. In announcing the voluntary safeguards, President Biden emphasised that the US will work with allies and partners to establish a strong international framework to govern the development and use of AI.[17]

# 5. Public sector

CBA believes the fundamental principles that guide the approach towards AI regulation should be the same across the private and public sector, but noting that the approach taken to regulation might differ as private sector regulation should be included within existing regulatory frameworks, whereas public sector regulation may need to be more specific. A consistent approach will promote the public's trust and confidence in AI.

CBA notes recent recommendations, directed towards the public sector, related to the use of ADM that stem from the Royal Commission into the Robodebt Scheme, and believes such initiatives would support responsible AI practices across the public sector. Recommendation 17.1 (Reform of legislation and implementation) and Recommendation 17.2 (Establishment of a body to monitor and audit ADM) would impose check and balances, such as pathways for review, requirements around explainability and transparency which would mirror those currently in operation in private sector settings.

The initiatives noted in the Discussion Paper in relation to the DTA's guidance on public sector adoption of AI and the Office of the Commonwealth Ombudsman's Automated decision-making better practice guide also work to support responsible AI practices in its own agencies.

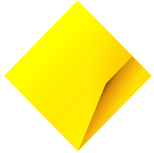
# 6. Transparency

CBA believes that transparency of outcomes, and the ability to explain decisions from AI applications has significant implications for public trust and confidence in AI technologies. This point is well established in the Discussion Paper.

---

[16] https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/21/fact-sheet-biden-harris-administration-secures-voluntary-commitments-from-leading-artificial-intelligence-companies-to-manage-the-risks-posed-by-ai/
[17] https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/21/fact-sheet-biden-harris-administration-secures-voluntary-commitments-from-leading-artificial-intelligence-companies-to-manage-the-risks-posed-by-ai/





In many cases, AI will support a 'human in the loop' decision maker and adoption of AI should have no obvious impact on the rights of affected persons. In this context, it is essential that the human decision maker in question understands the basis upon which the AI has contributed to, or informed, the final decision and this necessitates transparency. We acknowledge that there are circumstances where AI and ADM can be implemented without a 'human in the loop'.

To support the fair use of AI, it is important that entities adopt appropriate explainability techniques. Explainability enables a model developer to explain what happens in a model from the input phase to the output being generated.

Explainability is essential as it is a necessary pre-requisite supporting transparency, compliance and, ultimately, trust. The actual techniques adopted will depend on the circumstances. For example, an intrinsically explainable model involving linear or logistic regression requires different approaches to a model using deep learning. Other relevant considerations are whether there is a 'human in the loop' and the purpose for which the model is being used (e.g. a recommender engine versus a decision impacting the supply of services). The notion of explainability should also extend to model developers being able to describe the steps they have taken to ensure the data used in the model has been used in a fair manner.[18] There is a large body of existing work that model developers can use for this purpose.

CBA considers that any centralised entity focused on the coordination of AI regulatory issues could play a leading role ensuring that better practice guidance was shared across the economy and at the sector level, as appropriate.

With regard to mandating explainability or transparency requirements, we believe that the AHRC Report Recommendation 10[19] and Recommendation 11[20] go too far but agree that caution is advised when decision-making affecting fundamental rights is carried out without human oversight and control.

In order to avoid unnecessary complexity and reduce the regulatory burden on entities, CBA also believes that any Australian framework should not duplicate existing legislative requirements. For example, under existing Australian privacy law and according to Australian Privacy Principle 5, entities already have general transparency obligations to notify individuals about how their personal information will be used.

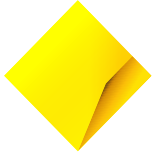
In addition, greater transparency measures are considered under the Privacy Act Review Report, including the proposed right to object (Proposal 18.2), and the right to request meaningful information about how automated decisions are made (Proposal 19.3). CBA did not support Proposals 19.1 and 20.9 due to concerns about commercial sensitivities and whether increasing the complexity of privacy policies and notices would actually result in meaningful transparency. These arguments are set out in our March 2023 public submission to the Privacy Act Review Recommendations.

# 7. High-risk applications

CBA believes that the majority of risks posed by AI can be managed by a principles and risk-based approach with strong governance and appropriate controls using existing frameworks.

[18] For example, identifying and quantifying whether disparity exists, including metrics for demographic parity, disparate impact and treatment, differential validity, proxy discrimination, and equality of opportunity.
[19] AHRC, The Human Rights and Technology Final Report (2021), Recommendation 10: The Australian Government should introduce legislation to require that any affected individual is notified when a corporation or other legal person materially uses AI in a decisionmaking process that affects the legal, or similarly significant, rights of the individual.
[20] AHRC, The Human Rights and Technology Final Report (2021), Recommendation 11: The Australian Government should introduce legislation that provides a rebuttable presumption that, where a corporation or other legal person is responsible for making a decision, that legal person is legally liable for the decision regardless of how it is made, including where the decision is automated or is made using artificial intelligence.





In a few limited cases, there may be specific circumstances in which bans on AI may be appropriate where the risk is not appropriately dealt with by existing law. These areas are unlikely to be unique to Australia and international developments are illustrative in terms of when AI might be prohibited. For example, in the US, legislation exists to prevent insurers and hiring organisations from using data in a way that unfairly discriminates customers based on race and other grounds. In the EU, the AI Act prohibits specific AI practices entirely, including technologies that:

- deploy subliminal techniques beyond a person's consciousness to materially distort a person's behaviour in a manner that causes or is likely to cause harm;
- exploit vulnerabilities of a group due to their age, physical or mental disability to materially distort the behaviour of a person pertaining to that group in a manner that causes or is likely to cause harm; or
- evaluate or classify the trustworthiness of natural persons based on their social behaviour or known or predicted personal or personality characteristics, leading to detrimental or unfavourable treatment.[21]

The EU Act also proposes bans on use cases that pose an 'unacceptable' risk to human rights, including rights to non-discrimination and privacy. While CBA broadly supports the objectives of these international developments, we reiterate that Australian legislators should carefully consider duplicating obligations that exist under existing frameworks. For example, as per existing Australian privacy law, circumstances in which AI or automated decision-making are not appropriate already include those use cases that are not within an individual's reasonable expectations of how their personal information will be used. This includes where AI is likely to cause harm to the individual (whether that harm be financial, reputational, psychological or physical).

It should also be noted that given the global nature of AI development, banning use cases in the Australian context will not stop bad actors from developing and implementing these use cases internationally, and may only result in overregulation of Australian companies.

# 8. Public trust

As the Discussion Paper emphasises, building public trust and confidence in AI involves consideration of whether further regulatory and governance responses are required to ensure appropriate AI safeguards are in place.

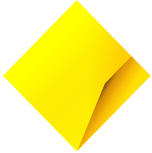
While CBA maintains that existing regulatory frameworks are appropriate, we note recent evidence presented by the University of Queensland and KPMG (discussed earlier) to suggest that the community believes these frameworks are insufficient.

Globally, three out of five people are wary of trusting AI systems and report either ambivalence or an unwillingness to trust AI technologies. While 82% of people are aware of AI, half of these people report that they do not understand AI and do not know when or how it is being commonly used.[22] This presents a significant issue for government and industry alike towards the greater adoption and acceptance of AI. People who understand AI are more likely to accept it and perceive benefits about its use. This suggests understanding AI sets a foundation for trust. Significantly, 82% or people want to know more about AI, which suggests when considered together, there is a strong need and appetite for public education on AI and the governance arrangements that protect consumers from perceived harm.[23]

---

[21] https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence
[22] https://ai.uq.edu.au/files/6161/Trust%20in%20AI%20Global%20Report_WEB.pdf
[23] This view is supported by a separate study by Monash Data Futures Institute which shows that many people will change their initial opinions and preconceptions about AI when provided with further information, examples and questions -





Activities proposed in the UK's current inquiry include regulators promoting awareness raising campaigns to educate consumers and users on AI regulation and risks, and guidance from regulators to businesses seeking to navigate the AI regulatory landscape. CBA would welcome similar initiatives in the Australian context leveraging the foundational work led by the Australian Government in establishing Australia's Eight AI Ethics principles that build consumer trust. Bodies such as CSIRO's National AI Centre could play a leadership role in building public trust of AI, which is currently focused on building capabilities, attracting new investment, and addressing barriers for small and medium sized businesses.[24]

Ultimately, CBA believes that trust in AI will be amplified where the public can see that AI can improve services, deliver better outcomes, and not create harm. As such, the regulatory and enforcement regime should champion examples where human benefit is created, and quickly act to address consumer harms that emerge.

# 9. Implications and infrastructure

In relation to infrastructure and information security, AI services should be considered the same as a traditional 'application layer code'. As such, CBA believes existing industry standards around information security, data protection and infrastructure should continue to apply to the systems that underpin AI services, including data hosting and sovereignty considerations.

# 10. Risk-based approaches

CBA strongly believes that the majority of risks posed by AI can be managed by a principles and risk-based approach with strong governance and appropriate controls. A risk-based approach to AI is beneficial as it can enable companies and regulators to keep up with the pace of innovation.

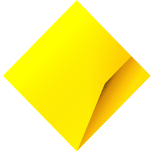
The limitations of risk-based approaches primarily relate to the finite resources that companies have to manage all risks. Managing all risks will not always yield the best results. Resources should be directed to the highest risk items where there is potential for large impacts on consumers. Although this could result in more undesirable outcomes on the lower risk items, this is far more palatable, as the impact of these would not be material. In order to successfully calibrate a risk-based approach that results in the higher risks being effectively mitigated, organisations need to ensure:

- They have a good understanding of the potential adverse consequences of an AI
- That they risk-rate the scenario appropriately, taking into account both the likelihood and the consequence of the unexpected behaviour;
- That the risk rating is revised each time the AI is applied to a different use case (as the same AI may be used for both immaterial or material applications, and these scenarios need to be risk managed differently even though it is the same AI); and
- Immaterial risk model risk ratings continue to be reviewed periodically to ensure the materiality has not changed over time.

file:///C:/Users/bowtelda/Downloads/AI%20for%20Social%20Good%20-%20Australian%20Attitudes%20Toward%20AI%20and%20Society%20Report.pdf

[24] https://www.industry.gov.au/news/national-artificial-intelligence-centre-launched





# 11. Conclusion

Australia has strong foundations to be a leader in the application of safe and responsible AI. Optimising the regulatory and governance measures to mitigate the potential risks from AI will increase public trust and confidence in AI's development and use.

CBA supports a technology neutral, principles led, and risk-based approach to regulation governing AI technologies. We believe that the vast majority of risks associated with AI are already appropriately regulated under existing frameworks and welcome greater guidance and coordination from government as to how organisations using AI technologies can conform to existing laws and regulations that govern data protection, privacy, consumer protection, discrimination, competition, and corporations across industries, as well as relevant sector-specific regulations.

The Government's consultation is an important step in developing the regulatory frameworks that will govern AI technologies that will be so critical towards enhancing Australia's productivity and economic prosperity.

CBA welcomes the opportunity to engage further with the Australian Government on the issues raised in this submission.