KPMG

Automated Decision Making and AI Regulation

Issues Paper

May 2022

Contents

01

Executive Summary

Executive Summary

KPMG Australia (KPMG) welcomes the opportunity to provide a submission to the Digital Technology Taskforce's Issues Paper on Automated Decision Making and Artificial Intelligence Regulation (the Issues Paper).

JAMES MABBOTT
Partner in Charge, KPMG Futures
KPMG Australia

KATE MARSHALL
Head of KPMG Law
KPMG Australia

As the Issues Paper notes, the safe and responsible development and deployment of new and emerging technologies like artificial intelligence (AI) and automated decision making (ADM) presents significant opportunities such as improvements in productivity and facilitating economic growth, among many others. In order to fully harness the opportunities these technologies present, Australia's regulation and regulatory systems must remain fit for purpose and agile.

Appropriate legal and regulatory frameworks are critical to providing individuals, businesses and government with increased certainty about the risks and benefits of adopting AI and ADM technologies, which in turn will encourage increased uptake and investment.

KPMG's research finds that the community's trust in AI systems strongly impacts the acceptance and adoption of the technology.[1] If AI is not developed and used in a trustworthy manner, it is likely that its full potential will not be realised. Further, the perceived adequacy of current regulations and laws is one of the strongest drivers of trust in AI systems, highlighting the importance of the right regulatory settings.

In this submission KPMG recommends that the Digital Technology Taskforce develop an enforceable regulatory framework for AI and ADM that builds on existing frameworks such as privacy and consumer laws, as well as identify a regulatory body to be responsible for enforcing the legislation. To ensure a fit for purpose framework, these regulations should be developed through a full industry consultation process, reviewed regularly, and be as technology neutral as possible. Additionally, the Digital Technology Taskforce could consider whether the AI Ethics Framework should be codified, to help ensure that those who benefit from AI are subject to the burden of proof that their technology is compliant and also have a clear understanding of their obligations. This will help both discourage detrimental applications of the technology while providing certainty to drive innovation.

This submission outlines 13 recommendations at section one and directly addresses the consultation questions at section two.

If you would like to discuss the contents of this submission further, please do not hesitate to reach out. KPMG looks forward to continued engagement with the Digital Technology Taskforce as is develops possible reforms and action on this issue.

[1] https://home.kpmg/au/en/home/insights/2020/10/artificial-intelligence-trust-ai.html

Background

About KPMG

KPMG is a global organisation of independent professional firms, providing a full range of services to organisations across a wide range of industries, governments and not-for-profit sectors. We operate in 146 countries and territories and have more than 227,000 people working in member firms around the world. In Australia, KPMG has a long tradition of professionalism and integrity combined with our dynamic approach to advising clients in a digital-driven world.

02

Recommendations

KPMG Recommendations

1

Recommendation 1

The successful adoption of AI can be assisted by addressing the public's current lack of trust in AI by ensuring regulations and laws are sufficient to ensure AI use is safe.

2

Recommendation 2

The development and adoption of a simplified and interoperable regulatory framework for AI should be accompanied by the identification of a leading regulatory body responsible for developing and enforcing AI legislation.

3

Recommendation 3

The Digital Technology Taskforce consider areas that are already subject to regulatory oversight, and ensure that the rights, duties and powers created by those regimes are appropriately adapted or modified to account for the problems unique to AI and ADM.

4

Recommendation 4

Develop an enforceable regulatory framework and certification regime for the responsible and human-centric development, deployment and use of AI and ADM.

5

Recommendation 5

To ensure a fit for purpose regulatory framework that reflects the most recent advancements in technology, regulations should be developed through a full industry consultation process and reviewed regularly. This will help maintain the right balance between innovation and safety.

6

Recommendation 6

Changes to the regulatory framework should aim to be as technology neutral as possible, to ensure it applies more appropriately both to AI and ADM but also future advancements in technology.

7

Recommendation 7

The Digital Technology Taskforce could consider whether a regulatory sandbox environment, looking at any key learnings from the Enhanced Regulatory Sandbox, could facilitate innovation in AI and ADM.

8

Recommendation 8

There is a need for new regulation with clear objectives to minimise the risks of AI and ADM, encourage their benefits and ethical use, and foster trust through accountability and transparency.

9

Recommendation 9

The Digital Technology Taskforce should consider whether compliance with the Artificial Intelligence Ethics Framework should be mandatory and provide guidance on how this framework should be implemented in practice. This type of framework could help to ensure that those who benefit from AI are subject to the burden of proof that their models are compliant, discouraging detrimental applications of the technology.

10

Recommendation 10

KPMG considers the use of AI and ADM in activities such as profiling of customers, marketing initiatives, and direct marketing, can certainly be detrimental if not used correctly and therefore it is critical that there is a strong regulatory framework around these settings and uses.

11

Recommendation 11

KPMG considers that there is merit in considering if there are uses of AI and ADM that are inherently inconsistent with Australia's position as a liberal democracy because of the risk such uses pose to the rights and fundamental freedoms of individuals as well as potentially to their safety.

12

Recommendation 12

Greater consistency with international regulatory frameworks would significantly reduce administrative burden, help with exporting technology out of Australia and set clearer expectations for the importation of technology.

13

Recommendation 13

Given the mature stage of development of the European Union's AI Act, Australia could consider the risk-based approach with stricter regulation of AI and ADM applications in high-risk areas, to inform its own regulation.

03

KPMG Insights

Response to consultation questions

1. What are the most significant regulatory barriers to achieving the potential offered by AI and ADM? How can those barriers be overcome?

Without public confidence that AI is being developed and used in an ethical and trustworthy manner, it will not be trusted, and its full potential will not be realised.[2] To echo the sentiment of Dr Alan Finkel AO, Australia's former Chief Scientist, acceptance of AI rests on "the essential foundation of trust".[3]

KPMG's research confirms that trust strongly influences AI acceptance. There are four key drivers that influence citizens' trust in AI systems:

1. Beliefs about the adequacy of current regulations and laws to make AI use safe;
2. The perceived uncertain impact of AI on society;
3. The perceived impact of AI on jobs; and
4. Familiarity and understanding of AI.

Of these drivers, the perceived adequacy of current regulations and laws is the strongest, demonstrating the importance of developing adequate regulatory and legal mechanisms that people believe protect them from the risks associated with AI use.[4]

While the law has historically lagged behind technological advancements, the scale and severity of the threats posed by uncontrolled AI represent an opportunity for regulators, policy makers and the broader AI eco-system to collaborate and rethink the approach to developing and enforcing laws in relation to data and the use and application of technology as well outcomes.

While most Australians believe the benefits of AI are either greater than or equal to the risks, the majority also view the societal impacts of AI as uncertain and unpredictable. Furthermore, most Australians believe the challenges associated with AI such as fake online content, surveillance, data privacy, cyber security, bias, technological unemployment and autonomous vehicles, are likely to impact a large number of Australians.

The Australian public are near unanimous in their expectation that the government and the companies deploying AI carefully manage these challenges, and that existing regulators should take the lead in regulating and governing AI systems.

Believing that AI regulation and laws are sufficient to make AI safe and protect affected stakeholders from the risks, is a key determinant of Australians' trust in AI systems. KPMG's 2020 report *Achieving Trustworthy AI*[5] found that almost all Australians (96 per cent) expect AI to be regulated, but most either disagree (45 per cent) or are ambivalent (20 per cent) that current regulations and laws are sufficient to make the use of AI safe and protect people from the risks. Most Australians expect external regulatory oversight by the government or regulatory bodies, with coregulation by government and industry also popular.

One of the key challenges for private and public organisations in the deployment and use of responsible AI resides in the multiplicity of guidelines, good practices and toolkits developed by the Australian Government as well as national and international policy makers. The development and adoption of a simplified and interoperable regulatory framework for AI should be accompanied by the identification of a leading regulatory body responsible for developing and enforcing AI legislations.

Recommendation 1
The successful adoption of AI can be assisted by addressing the public's current lack of trust in AI by ensuring regulations and laws are sufficient to ensure AI use is safe.

Recommendation 2
The development and adoption of a simplified and interoperable regulatory framework for AI should be accompanied by the identification of a leading regulatory body responsible for developing and enforcing AI legislation.

[2] https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai, https://acola.org/hs4-artificial-intelligence-australia/
[3] https://www.chiefscientist.gov.au/news-and-media/ai-can-we-get-it-right-please, https://www.weforum.org/agenda/2018/05/alan-finkel-turing-certificate-ai-trust-robot/
[4] https://home.kpmg/au/en/home/insights/2020/10/artificial-intelligence-trust-ai.html
[5] https://assets.kpmg/content/dam/kpmg/au/pdf/2020/achieving-trustworthy-ai.pdf

2. Are there specific examples of regulatory overlap or duplication that create a barrier to the adoption of AI or ADM? If so, how could that overlap or duplication be addressed?

Yes, there are areas where existing and overlapping regulation that impacts on the deployment and operation of AI and ADM. However, it is not necessarily the case that existing regulation per se creates a barrier to adopting AI or ADM. Rather, the existing legislative frameworks are not adequately adapted to the use of these technologies and their potential adverse impacts. They are therefore not directed to providing the right regulatory settings to effectively prevent the harms that can arise from their use, or to provide guidance and certainty for entities developing or using the technologies and afford individuals or groups of individuals with appropriate rights in relation to the data inputs and the outcomes of the use of AI and ADM as well as assurance, monitoring and oversight.

The current regulatory frameworks are directed at different inputs and outputs, and only surveillance devices legislation is directed at the use of devices that involve technology. None of them include, for example, a definition of AI or ADM or are stated to expressly apply to the use of AI or ADM.

Privacy Act

The *Privacy Act 1988* (Cth), through the Australian Privacy Principles (APPs), regulates the processing or handling of 'personal' including 'sensitive' information that may be inputs into AI and ADM. Australia has adopted the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and is a signatory to the International Covenant on Civil and Political Rights. These commitments are reflected in the Privacy Act. While there are no express rules in the APPs governing the use of AI to process or apply ADM using personal information, the APPs regulate the collection, use and disclosure of personal information which may be processed by AI or used for the purposes of ADM, including the requirement to obtain consent in certain circumstances.

For example, the Office of the Australian Information Commissioner (OAIC) has used its regulatory powers to investigate Clearview Inc's use of AI powered software to transform facial images available on social media sites into biometric templates that allow for photo-matching. The investigation found that Clearview breached APPs 1, 3, 5, and 10 as it would not have been able to collect the data lawfully, did not provide consent or notice, and had not validated the accuracy of the information.

APP10 imposes data quality obligations on organisations and agencies using personal information in AI and ADM platforms. This provision requires that such organisations ensure that personal information collected, used and disclosed is accurate, complete and up to date, having regard to the purposes for which it is used or disclosed. This is an important obligation in the context of AI and ADM and the quality of the training data sets that may be used. Individuals may also request correction of their personal information (APP13). However, this does not apply to the correction or review of ADM outcomes based on incorrect data. In contrast, Article 22 of the European *General Data Protection Regulation* (GDPR) gives individuals the right 'not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning [them] or similarly significantly affects [them]'. We note, however, that the definition of ADM in the Issues Paper is far broader than the relatively limited protections provided in the GDPR. First, the Issues Paper extends ADM to decision making made 'in whole or part' by automated means, whereas the GDPR protections only apply to solely automated decisions. Second, there are exceptions to the GDPR protections including where individuals consent, or if it is necessary to perform a contract the individual has entered with the organisation who is the 'data controller'. In such cases, the data controller must at least give the individual the right to have human intervention and to express his or her point of view and to contest the decision.

The Australian Consumer Law (ACL)

The ACL's misleading and deceptive conduct regime may apply where organisations make statements and representations about the collection and use of personal information, for example in their privacy policies and collection notices, that do not accurately reflect how AI may transform customer data and enable its use for secondary purposes, or how the data may be used for the purposes of ADM which produces certain outcomes. Further, the aggregation of multiple datasets may change non-personal information into personal information. For instance, if an algorithm compares products that are not sufficiently similar and provides a misleading or deceptive representation to consumers, it may enliven the provisions of the regime. The ACCC's Digital Platforms Services Inquiry March 2022 Interim Report has identified instances where inaccurate price comparisons constituted misleading or deceptive conduct. Similarly, the September 2021 Report identified the way 'dark patterns'[6] can be misleading or deceptive and thus harmful to individuals. These instances were directed by algorithmic behavioural analysis. However AI, in particular recursive machine learning models, has the potential to significantly increase the efficacy of behavioural analysis and manipulation, thereby potentially increasing the harm caused, while simultaneously making detection harder. Importantly, as an intention to mislead or deceive does not have to exist, organisations may not be able to escape liability by blaming the algorithm. The ACL regime could also apply to representations made about the purposes for which data is collected and used for the purposes of making the decisions in question.

Anti-discrimination laws

Commonwealth and state/territory discrimination laws in principle apply to decisions made via AI and ADM. These laws prohibit discrimination based on certain 'protected attributes' such as age, race, sex, and disability. Decisions that have a consequence for individuals and actions by government and businesses will need to comply with these laws.

Surveillance devices laws

Federal and state surveillance devices legislation governs the installation, use and maintenance of tracking, listening, optical and data surveillance devices by law enforcement agencies, private sector organisations, and employers. They broadly require consent to use such devices and contain some safeguards around privacy, including on the communication of information collected from these devices. However, this legislation was drafted with a focus on on-premises devices, while the use of AI is less dependent on physical proximity and can have downstream outcomes which are not sufficiently addressed by the existing legislation.

An approach to AI/ADM regulation

This lack of a clear legislative framework inhibits adoption in two important ways. First, entities that are developing AI/ADM platforms (AI/ADM Developers) and that seek to deploy AI/ADM (AI/ADM End Users) in their operations do not have sufficiently clear guidance about their compliance obligations. Second, individuals cannot have confidence that the development and use of AI/ADM will have the necessary safeguards, oversights and scope for appropriate rights and remedies including for example right of review or human intervention.

There are three key aspects to consider:

- Whether legislative intervention specifically targeting AI and ADM is the most appropriate approach – or whether the better approach is to more effectively calibrate existing regulatory environments to facilitate the adoption of trustworthy AI and ADM systems.
- The existing areas of regulation that, in our view, warrant consideration by a discussion paper for legislative reform.
- Options for trust-building measures for further consideration. These include licencing, auditing, impact assessment and regulatory oversight that can prevent the potential harms poorly deployed AI and ADM can create.

[6] Defined by the ACCC as 'an interface designed to deceive a user into performing actions they did not intend to undertake'

KPMG suggests that further consideration be given to whether a single "AI Act" is the most effective way of achieving the objectives described in the Issues paper. It is certainly the case that the current regulatory system is incomplete and fragmented. The European Union (EU) Commission, as part of its broader legislative strategy for data and digital services, has released a proposed regulation for AI called the *Artificial intelligence Act* (the EU AI Act). Similar to the GDPR, this legislation would introduce an EU wide framework regulating the development, deployment and use of AI and ADM systems – including creating additional supervisory and oversight bodies. This approach has the advantage of consolidating AI/ADM specific rules into a single place, and to the extent that such technology warrants bespoke rules then this makes sense. However, it is not necessarily the case that this means an omnibus AI Act is the most appropriate response for Australia, for several reasons, discussed below.

KPMG believes any legislative intervention should be tailored to ameliorate the specific harm. The concern about AI and ADM is the potential for these technologies to create harms – prevention of which is a key objective behind legislative intervention. However, any sufficiently complex algorithmic system can create harms irrespective of whether it employs AI or ADM. This has been identified from the research and ongoing reports of the ACCC's Digital Platform Services Inquiry. For example, the March 2022 report[7] that discussed the operation of general online retail marketplaces, identified harms to both consumers purchasing from such marketplaces, and sellers using hybrid marketplaces (i.e., those where their products compete with those offered by the marketplace operator). Such services may use complex algorithmic systems to display products for sale. However, such systems fall outside many definitions of AI. We note in this respect that the Issues Paper, while adopting a very broad definition of AI, still excludes from that definition 'mathematical algorithms that enable a computer to learn from text, images or sounds.' Adopting a risk- or harm-focused regulatory approach avoids definitional contests and focuses on the impact that the technology has on individuals and the market.

An alternative to an AI Act could be to identify areas that are already subject to regulatory oversight, and ensure that the rights, duties, and powers created by these regimes are appropriately adapted or modified to account for the problems unique to AI/ADM (or indeed any complex system). In particular, this would require consideration about what powers and resources would need to be given to the relevant regulators (i.e., ASIC, TGA, ACCC and the OAIC) to enable them to regulate activities to prevent and respond to harmful uses of AI/ADM. Creating a standalone AI Act would potentially create regulatory duplication that the Issues Paper implicitly wants to avoid. In this respect it is worth noting that even though the EU Commission has proposed a stand-alone Act, it is subject to the existing privacy law regulatory framework (i.e., the GDPR) and sectoral regulations.

Recommendation 3
The Digital Technology Taskforce consider areas that are already subject to regulatory oversight, and ensure that the rights, duties and powers created by those regimes are appropriately adapted or modified to account for the problems unique to AI and ADM.

[7] https://www.accc.gov.au/focus-areas/inquiries-ongoing/digital-platform-services-inquiry-2020-2025/march-2022-interim-report

3. What specific regulatory changes could the Commonwealth implement to promote increased adoption of AI and ADM? What are the costs and benefits (in general terms) of any suggested policy change?

While the perceived adequacy of current regulations and laws to govern AI is the strongest driver of citizens' acceptance of AI, current regulations are deemed insufficient to make the use of these systems safe for individuals and society. According to KPMG's research, more than 70 per cent of Australians would be more willing to use AI systems if assurance mechanisms were in place. In KPMG's view the primary regulatory objective should not solely be to promote increased adoption, but to ensure that beneficial applications are encouraged, and detrimental applications are discouraged.

Additional considerations and more specific regulatory changes could include:

1. Regulation to ensure data privacy of the consumer / customer / Australian public whose information is collected, stored and used to develop AI solutions, as per KPMG's submission to the Review of the Privacy Act.[8]
2. Guidelines on the appropriate use of AI as well as standards on identifying and measuring unintended consequences of AI implementations such as bias and discrimination. This could include areas where all organisations are required to monitor and report on unintended bias and discrimination, for example based on gender or ethnicity, as well as other areas that may be specific to particular organisations.
3. Transparency and accountability in the development and use of AI technologies in a manner that is consistent with user expectations, organisational values and societal laws and norms.
4. Clearer regulations on the intellectual property (IP) status of publicly available data being used for development and training of AI models, including consideration being given to legislating for a database right.
5. Regulation on IP ownership of AI systems in relation to opensource algorithms and ownership of the data being used in their development.
6. Clarification on the ownership of IP being created by AI systems.
7. Implementation guidance on appropriate regulatory safeguards for organisations to ensure outcomes are fair, unbiased, explainable and auditable. This regulatory guidance should be technology neutral.
8. A tiered system of mandatory requirements could be considered for high-risk sectors and lower-risk sectors.

In terms of cost-benefit analysis of these measures, the Issues Paper highlights why Australia values AI and ADM – namely, the potential for "improvements in productivity, facilitating economic growth and high-quality jobs, improving our health, raising our living standards, protecting the environment and improving our defence and national security capabilities". Regulation that effectively enhances the likelihood of achieving these benefits with a feasible cost of implementing the regulation is worthwhile. Any AI or ADM application which cannot demonstrate how it contributes to positive societal outcomes, such as those listed above, is at risk of generating societal cost, without sufficient societal benefit. Looking to international examples, the proposed EU AI Act requires AI and ADM applications in high-risk areas to be actively approved in a conformity assessment, before it can be implemented.[9] It may be worth considering whether aligning to this approach would be a suitable pathway for Australia to follow, while also considering any local nuances, for example in the specific approach to the conformity assessment, which could leverage the existing AI Ethics Framework.

Recommendation 4
Develop an enforceable regulatory framework and certification regime for the responsible and human-centric development, deployment and use of AI and ADM.

[8] https://home.kpmg/au/en/home/insights/2022/01/review-privacy-act-1988-kpmg-submission.html
[9] https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

4. Are there specific examples where regulations have limited opportunities to innovate through the adoption of AI or ADM?

While defining appropriate guardrails to ensure the safe adoption of AI and ADM technologies is essential, regulations need to achieve the right balance and stay up to date with the advancement of technologies to avoid excessive limitations and unrealistic expectations.

Examples of this include the unclear definition of explainability, and trying to enforce expectations of more conventional rule-based methods to the new techniques. Existing regulations in the financial industry, for example, require predictive risk models to be explainable to supervising bodies and are approved after human review of the logic. This approach has worked well with more conventional methods like logistic regression based on a limited number of data points. However, when it comes to complex models based on thousands of variables and methods like artificial neural networks, it won't be possible to explain them in the conventional form of human language rules. This has significantly limited the adoption of many of these techniques, even if they have proved to be more accurate and efficient through suitable and explainable scientific tests.

This demonstrates that fit for purpose regulation is essential to unlocking the innovation and benefits that technology advancements can provide. To minimise the limitations that regulatory frameworks can create, KPMG considers that regulations should be developed in consultation through a full industry consultation process, reviewed regularly, and aim to be as technology neutral as possible.

Recommendation 5
To ensure a fit for purpose regulatory framework that reflects the most recent advancements in technology, regulations should be developed through a full industry consultation process and reviewed regularly. This will help maintain the right balance between innovation and safety.

5. Are there opportunities to make regulation more technology neutral, so that it will apply more appropriately to AI, ADM and future changes to technology?

KPMG considers that it is critical to adapt current regulation in order to make it technology neutral. Technology is evolving at a rapid pace and therefore legislation must remain agile to adapt to these future advancements. By creating a more technology neutral legislative and regulatory framework, it will also apply more appropriately to AI and ADM.

Recommendation 6
Changes to the regulatory framework should aim to be as technology neutral as possible, to ensure it applies more appropriately both to AI and ADM but also future advancements in technology.

6. Are there actions that regulators could be taking to facilitate the adoption of AI and ADM?

KPMG considers that the primary regulatory objective should be to ensure that beneficial applications of AI and ADM are encouraged, and more detrimental applications are discouraged. An idea that could be given further consideration is replicating a scheme such as the Enhanced Regulatory Sandbox (formerly the FinTech Regulatory Sandbox).[10] This scheme aims to create space for innovation and experimentation, with appropriate guardrails in place to safeguard against detrimental outcomes.

The financial industry was one of the first movers in AI and ADM. As an example, in March 2020, ASIC issued directions to reduce high frequency trading (HFT) by up to 25 per cent from the levels executed on 13 March 2020.[11] HFT algorithms can trade at a speed which humans cannot control or comprehend. In some situations, this is legitimate and helpful, such as when HFT algorithms trade on price differences between assets listed simultaneously in two different markets. Since there is no reason for prices for the same asset to differ between two markets, and it occurs due to inefficiencies in the speed of information dissemination, correcting this with HFT is desirable.

However, many algorithms profit from trading on volatility. This can create further volatility via these trades and then continue to profit from trading the self-perpetuating cycle of increased volatility. Individual market participants can earn profits from this, but it is detrimental for the market and broader society as financial market volatility creates real economic uncertainty, not to mention transaction costs. This is a complex topic, which ASIC has been investigating since 2012. The most recent report suggests that the costs of HFT have decreased from previous highs, though there is yet to be an update since the outbreak of the pandemic.[12]

This example highlights that encouraging beneficial applications of AI and ADM is desirable and that it is vital to be able to rationally explain what real world problem an AI or ADM application is solving. If not, it may present risk or detriments to society, with benefits accruing only to certain actors.

The Digital Technology Taskforce could learn from the path trodden by the finance industry and seek to proactively introduce a forum such as the Enhanced Regulatory Sandbox. This would provide a transparent mechanism to exemplify the real-world problems being solved by AI and ADM mechanisms and validate that no negative unintended consequences are being generated in the process. When considering this type of scheme, there would also need to be clear specifications around the data being used.

Recommendation 7
The Digital Technology Taskforce could consider whether a regulatory sandbox environment, looking at any key learnings from the Enhanced Regulatory Sandbox, could facilitate innovation in AI and ADM.

[10] https://asic.gov.au/for-business/innovation-hub/enhanced-regulatory-sandbox/enhanced-regulatory-sandbox-exemption-users/
[11] https://asic.gov.au/about-asic/news-centre/find-a-media-release/2020-releases/20-062mr-asic-takes-steps-to-ensure-equity-market-resiliency/
[12] https://download.asic.gov.au/media/4941728/rep598-published-19-november-2018.pdf

7. Is there a need for new regulation or guidance to minimise existing and emerging risks of adopting AI and ADM?

As outlined throughout this response, there are clear benefits and risks associated with the adoption of AI and ADM that have likewise been identified internationally and in Australia. As the technology evolves at an increasing pace, society's expectations to both utilise and control it grow.

Responses to this challenge are evolving, with ethics frameworks and guidelines being developed for the public and private sector. These, in turn, are being translated into legislative frameworks, particularly in the European Union and through standards setting bodies like the International Standards Organisation (ISO) and Institute of Electrical and Electronics Engineers (IEEE). These standards are often then introduced into domestic legislative settings.

It is, therefore, natural to expect the development of new regulation and underpinning guidance to be developed in Australia to encourage the economic and social benefits of AI and ADM adoption, while seeking to mitigate its growing risks. It is this dual objective that should form the basis of a regulatory framework and continue to guide the government's work in this space.

In particular, in regulating any new AI or ADM applications, products or services, their risks should be clearly articulated, mitigation measures clearly identified and subsequent monitoring, compliance and enforcement mechanisms established.

Accountability governance and risk mechanisms

AI accountability refers to the expectation that organisations will ensure the proper functioning of AI systems in accordance with their roles and applicable regulatory frameworks. Such frameworks can be prescriptive or principles-based or a mixture of both. Given the ethical frameworks already developed, KPMG considers that a mixture would be useful to align principles with specific risk mitigating practices, including leveraging those that are already utilised in the private sector and other comparable regulatory regimes.

Organisations developing or using AI systems, whose outcomes may impact on people, usually carry out risk and impact assessments and put in place appropriate risk management processes. Where possible, organisations should leverage existing governance and risk frameworks and mechanisms, adapting these to cater for the expanded risks to the organisation and potential impacts on people from AI systems.

Establishing interdisciplinary governance boards to assess and govern AI-enabled operations, products and services is now best practice. For example, some companies have established a governance council, with senior executives and representatives from different business teams to review and approve the implementation of AI applications determined to be high risk.

In investigating an appropriate regulatory framework, KPMG considers that the government could usefully explore with industry:

- the development and adoption of a code of conduct or charter that embeds shared values and principles to support ethical and trustworthy data use and AI;
- how responsibility and accountability can be clearly defined, allocated, understood and executed across key stages of the AI lifecycle;
- the development of governance, monitoring and reporting structures that provide appropriate oversight of how AI systems and technologies are brought into an organisation's operations, products and/or services;
- transparently document who can, is and should be making key decisions throughout the AI system lifecycle;
- the development of an initial risk assessment and scoring system to determine an AI project's level of risk to business and to stakeholders upfront and ensure the appropriate level of governance oversight and remediation is applied;

- how to establish transparent and accessible processes for employees, customers and other stakeholders to report potential risks, biases or vulnerabilities in the AI system as well as potential breaches of future regulations;
- where AI systems are operating in critical functions with high risks to people, potentially impacted communities should be engaged, with a focus on the most vulnerable and marginalised stakeholder groups;
- consider a staged release of new algorithms that have the potential to impact many, to enable robust assessment of potential impacts prior to broader release; and
- review communication channels and interactions with stakeholders of AI systems to provide disclosure.

Managing Risk: How can standards and certifications help?

Regulated standards and certifications can facilitate the widespread adoption of trustworthy AI and help reduce risks. They can also enhance public trust by giving assurances that products that hold the certification have been tested and shown to meet technical performance and ethical standards.

Standards work in AI is being developed by international bodies such as the ISO and IEEE. For example, the IEEE P7000 series of standards projects aims to develop standards inclusive of both technological and ethical considerations.

The question for government and industry to subsequently consider is how these standards and certifications are implemented and by whom. For example, a regulator could certify AI or ADM software products or services based on data reports showing that the products make decisions or produce outcomes that conform to the desired ethical principles (e.g. are not biased or discriminatory) or other relevant criteria.

Regulation should instil trust through accountability and transparency to mitigate, for example, the scenario where the AI or ADM developer and/or owner benefit from it without responsibility for adverse consequences. For example, internet AI algorithms are used to show related content and advertising according to the user's algorithmically defined preferences to retain their attention.

This can lead to users being exposed to increasingly extreme content over time that they may not have initially sought and, in a worst case scenario, negatively alter their behaviour to effect those around them and wider society.

KPMG considers that the Digital Technology Taskforce could work with industry to develop a way to identify and classify negative consequences, as well as a means to distinguish between intended and unintended consequences. Regulatory frameworks can include mechanisms obligating organisations to implement processes to avoid negative outcomes. It also provides the opportunity to set a high standard of ethical behaviour and foster trust in the technology.

Recommendation 8
There is a need for new regulation with clear objectives to minimise the risks of AI and ADM, encourage their benefits and ethical use, and foster trust through accountability and transparency.

8. Would increased automation of decision making have adverse implications for vulnerable groups? How could any adverse implications be ameliorated?

To answer this question KPMG has identified vulnerable groups, potential adverse implications, and provided examples of appropriate mitigation actions. As noted above in Question 2, existing discrimination law provides some legal protections to certain groups. While such legal protections are critically important, they cannot be relied on alone to protect vulnerable groups from adverse effects and therefore need to be seen as a minimum standard. Preventing adverse impacts on vulnerable groups will also require AI and ADM Developers and AI/ADM End Users to take proactive steps to mitigate this risk. The following table summarises these points and highlights international examples of mitigation actions.

Vulnerable group	Potential adverse implication	Mitigation
Children	Violation of the UN Convention on the Rights of the Child	Apply UN policy guidance on AI for children
Minority populations (for example, race or gender minorities, whereby gender minorities may include females in certain contexts)	AI bias and its potential adverse impacts include: **1.** Data bias – when model training data represents past human discrimination, which is then replicated by an AI model and perpetuates discrimination **2.** Reporting bias – when minorities are insufficiently represented in training data, which means the needs of the minority population are either not served as well, or possibly even actively undermined by the application of AI **3.** Implicit bias – when minorities are insufficiently represented in developer groups, which means the needs of these populations are underserved by AI technologies	Different mitigations are required for different forms of bias: **1.** Data bias can be mitigated by requiring models to be tested against sensitive characteristics (for example, race, gender, sexual orientation, etc.) to provide evidence that the model does not discriminate on this basis (Note: It is insufficient to simply mandate that sensitive characteristics cannot be used in model training) **2.** Reporting bias can be mitigated by requiring training datasets to reflect the population to which AI and ADM will be applied **3.** Implicit bias can be addressed by encouraging minority populations to enter technical professions (for example women or those with Indigenous heritage, who are currently under-represented)

Vulnerable group	Potential adverse implication	Mitigation
Citizens with disabilities	• Above points relating to minority populations are also applicable here • Additional potential implications depend on specific nature of the disability, but include: • Disability impacting a person's appearance risks adverse implications for visual processing AI applications • Disability impacting a person's speech risks adverse implications for speech processing AI applications • Disability impacting a person's cognitive processing style or ability risks adverse implications for interactive AI applications	• Points relating to minority populations are also applicable here • Leading edge research on AI for people with disability (including recommendations to address issues) is being conducted by IBM Research
Technically remote populations (for example, senior or regional citizens)	Technologically remote citizens are more likely to 'miss out' on AI-related benefits, be it due to a lack of a suitable access device or internet connectivity, lack of prerequisite knowledge or due to a higher level of distrust	• Apply WHO Policy Brief on combatting ageism in AI for health • Additional measures unique to Australian regional populations are likely to be required, leveraging existing efforts to combat inequality in access to the NBN • Continue to invest in measures to build trust in AI, with a particular focus on technically remote populations

KPMG considers that investments should be made to counteract discrimination and potential adverse impacts for vulnerable groups. There are technically feasible ways to do so, as described in the mitigation details in the table above. In fact, since algorithms are not prone to sub-conscious or emotional bias as humans are, automating decision-making could be a way to reduce discrimination of vulnerable populations.

KPMG recognises that it is not feasible for regulators to mandate that every AI application provide proof of implementation for the above listed mitigation actions. Nonetheless, requiring compliance with the Artificial Intelligence Ethics Framework and providing guidance on how to implement it in practice would enhance developers' ability and incentive to comply.

This would significantly reduce adverse impacts on vulnerable populations, who currently have no effective mechanism to hold developers accountable for any adverse implications they may face because of increased use of AI and ADM.

Recommendation 9

The Digital Technology Taskforce should consider whether compliance with the Artificial Intelligence Ethics Framework should be mandatory and provide guidance on how this framework should be implemented in practice. This type of framework could help to ensure that those who benefit from AI are subject to the burden of proof that their models are compliant, discouraging detrimental applications of the technology.

9. Are there specific circumstances in which AI or ADM are not appropriate?

KPMG considers that there are certain circumstances where AI or ADM may not be appropriate, and where additional caution and strict regulatory guardrails are required. This would assist in ensuring that beneficial applications of the technology are encouraged, while potentially detrimental applications are discouraged.

The use of AI and ADM in activities such as profiling of customers, marketing initiatives, and direct marketing, can certainly be detrimental if not used correctly and therefore it is critical that there is a strong regulatory framework around these settings and uses.

As noted above, other specific circumstances where AI and ADM are not appropriate is when an individual developer stands to benefit, but broader society bears the risk and subsequent cost of unintended negative side effects. It is not realistic to expect to 'check' every single algorithm which is being developed. However, a framework such as the AI Ethics Framework, which is solidified in regulation, would help to ensure that those who benefit from AI are subject to the burden of proof that their decision models are compliant.

KPMG suggests that further consideration should be given to enforcement mechanisms. For example, if an operator cannot evidence regulatory compliance, they must compensate those who are unfairly impacted by their AI and ADM models as is the case under, for example, consumer protection and competition law. This means there must be an enforceable dispute resolution mechanism and remediation model for non-compliant AI and ADM applications.

We note that the proposed EU AI Act has adopted an approach of placing an absolute prohibition on certain uses of AI that the High-Level Expert Group consider to be unable to used in an acceptable way. These include AI systems that:

- use subliminal techniques beyond a person's consciousness in order to materially distort a person's behaviour;
- exploit any of the vulnerabilities of specific vulnerable groups in order to materially distort the behaviour of a person;
- are deployed by public authorities to give people a social credit score based on evaluations of individuals' their social behaviour or personality characteristics; and
- (with exceptions for emergencies) use of 'real-time' remote biometric identification for general law enforcement purposes.

KPMG considers that there is merit in considering if there are uses of AI/ADM that are inherently inconsistent with Australia's position as a liberal democracy because of the risk such uses pose to the fundamental rights and freedoms of individuals as well as potentially to their safety.

Recommendation 10
KPMG considers the use of AI and ADM in activities such as profiling of customers, marketing initiatives, and direct marketing, can certainly be detrimental if not used correctly and therefore it is critical that there is a strong regulatory framework around these settings and uses.

Recommendation 11
KPMG considers that there is merit in considering if there are uses of AI and ADM that are inherently inconsistent with Australia's position as a liberal democracy because of the risk such uses pose to the rights and fundamental freedoms of individuals as well as potentially to their safety.

10. Are there international policy measures, legal frameworks or proposals on AI or ADM that should be considered for adoption in Australia? Is consistency or interoperability with foreign approaches desirable?

New international policy initiatives focused on the governance of data and AI signal the end of self-regulation and the rise of new forms of oversight. It is likely that the years to come will be important for embedding regulations designed to govern AI on a global scale. Despite the increasing energy and efforts to accelerate the development of global AI regulations, the timelines to introduce internationally accepted and enforceable laws remain unclear. Additionally, the uplift of existing laws and regulations will require time to be fully formalised and implemented.

Although a more formal global regulatory framework will take time, KPMG considers that consistency and interoperability with international regulatory frameworks for AI and ADM would significantly reduce administrative burden and provide increased certainty for businesses and individuals in adopting these technologies. Greater consistency and interoperability will also make it easier to import and export technology due to clearer expectations. The developments in AI legislation in Europe, namely the development of the EU AI Act, could be considered as a starting point in Australia, particularly the EU's adoption of a risk-based approach to AI regulation.

Recommendation 12
Greater consistency with international regulatory frameworks would significantly reduce administrative burden, help with exporting technology out of Australia and set clearer expectations for the importation of technology.

Recommendation 13
Given the mature stage of development of the European Union's AI Act, Australia could consider the risk-based approach with stricter regulation of AI and ADM applications in high-risk areas, to inform its own regulation.

04 Key Authors

Key Authors

JAMES MABBOTT
Partner in Charge, KPMG Futures

KATE MARSHALL
Head of KPMG Law

KELLY HENNEY
Compliance & Conduct Leader, Privacy & Data Protection

DR SANJAY MAZUMDAR
Partner, Data & Cloud

ROBERT WARREN
National Leader, Risk Strategy & Technology

JACINTA MUNRO
Partner, Risk Assurance

DEAN GRANDY
Partner, Management Consulting

CRAIG DAVIS
Partner, Financial Risk Management

PHIL THORNLEY
Partner, Data & Cloud, Global Data/ Analytics & Emerging Technologies

ALI AKBARI
Artificial Intelligence Capability Lead – Innovation, Solutions & Ventures

VERONICA SCOTT
Cyber, Privacy & Data Lead, KPMG Law

SHUBHAM SINGHAL
Director, Compliance & Conduct, Privacy & Data Protection

DEAN LARSEN
Director, Compliance & Conduct, Privacy & Data Protection

DEAN GRANDY
Partner, Management Consulting

WILAN WONG
Director, Management Consulting

DANE ROBERTS
Director, Audit Assurance & Risk

ANNE CLERC-JOHNSON
Director, Compliance & Conduct

DR CHRISTINA KLEINAU
Data Platform Delivery Lead, Management Consulting

TANSEL ERAVAS
Associate Director, Management Consulting

SAM HARTRIDGE
Senior Manager, KPMG Law

MARK DUNNING
Manager, Compliance & Conduct, Privacy & Data Protection

LEAH ROY
Senior Consultant, Compliance & Conduct, Privacy & Data Protection

PETER KOMOCKI
Associate Director, Government & Regulatory Affairs

OLIVIA SPURIO
Senior Consultant, Government & Regulatory Affairs

KPMG.com.au

July 2022. 918128337DTL