



20 May 2022

Digital Technology Taskforce  
Department of Prime Minister and Cabinet

Dear Digital Technology Taskforce

## Positioning Australia as a leader in digital economy regulation – automated decision making and AI regulation

The Australian Banking Association (**ABA**) welcomes the opportunity to engage with the Digital Technology Taskforce on the automated decision making (**ADM**) and AI discussion paper, and the broader work program of the Taskforce.

Australian banks are using new technologies to increase efficiency and to provide new and more responsive services to customers. Banks have applied strong governance frameworks to the use of new technologies, and would be pleased to provide further information to the Taskforce about current practices.

### Key recommendations

In order to foster Australia's adoption of AI and ADM, ABA's key recommendations are:

- First focusing on simplifying or rationalising existing legislation that impact on the use of AI and ADM, in preference to new specific AI regulations. Specifically, consider guidance on the use of AI and ADM in compliance with the *Privacy Act 1988*.
- Any regulatory intervention including setting best practice guidance should build on existing best practices and harmonise with sector specific regulation.
- Review and amend legislation to be neutral as to whether a human or technology is used to make decisions or conduct a process.

Further comments and detailed recommendations are provided in the attachment.

If you have any queries, please contact me.

Yours sincerely,

Rhonda Luo  
Policy Director  
Australian Banking Association



## Comments and recommendations

### Context

ABA welcomes the Department of Prime Minister and Cabinet's consideration of Australia's regulatory settings and how they can support and enable the responsible use of new technologies, with a focus on AI and ADM.

The potential of AI and ADM may be realised across consumer goods, business and enterprise technology, research, enabling participation by citizens, creating innovative business opportunities. In the private sector, AI and ADM may facilitate customer-facing interactions, where they can be used to personalise the customer experience, in internal areas to improve efficiency or to support new types of services, and to enhance functions like fighting financial crime. Currently, the adoption of technology may vary significantly between groups of citizens or customers, between industries and even between entities – for example between online-only, 'brick and mortar' or hybrid business models. However, consumer preferences, cost and efficiency drives and other competitive dynamics may be expected to drive further adoption of AI and ADM.

An Australian government response to AI and ADM would come into an already crowded regulatory environment. Policy considerations about the use of AI and ADM touch on other areas of law and policy, such as data access, privacy, data ethics, competition law, and current regulatory debates such as the oversight of social media and digital platforms. In addition, sector-specific regimes may already regulate the use of technology. As a case in point, the banking industry is subject to comprehensive prudential and conduct regulations on all aspects of a bank's business, in addition to general legislation including the Privacy Act. Banks also occupy a privileged position of trust in the community. Reflecting these regulations and community expectations, banks have adopted robust governance processes for the use of technology including AI and ADM.

Overseas approaches to AI and ADM vary. The European Union (**EU**) is proposing AI Regulations and Rules on liability, to be followed by a review of specific EU regulation on machinery and product safety. US regulatory agencies are issuing guidance or taking other action to address AI and unlawful discrimination, and in specific areas like housing, employment and financial services. The Monetary Authority of Singapore and the Bank of England have engaged industry practitioners, researchers, educators and technologists as part of regulatory work including developing best practice guidance. Industry associations including the IIF are developing principles for their members on issues such as ethical use of customer data.

**ABA Recommendations:** In this context, ABA recommends:

- Government policy should consider AI and ADM as a whole-of-economy policy issue and as an enabler for economic activity, rather than a stand-alone policy issue or a new type of product or service.
- Foster the adoption of AI and ADM by first focusing on simplifying or rationalising existing legislation that impact on the use of AI and ADM, in preference to new specific AI regulations.
- Any regulatory intervention including setting best practice guidance should be based on open dialogue between regulators, policymakers and industry stakeholders, build on existing best practices and harmonise with sector specific regulation.

### Considering general legislation

#### Gap analysis and existing legislation

ABA welcomes the Government's proposal to build on existing work that has been done on the application of existing legislation and regulatory regimes to AI and ADM. ABA also supports the Government working with industry to identify principles that should underpin any further work on digital and technology.



ABA strongly supports these initiatives seeking to promote consumer confidence and mitigates poor consumer outcomes, without being too prescriptive and hampering the evolution and adoption of new technologies. Absent the gap analysis described below, ABA does not see a case for new general legislation to regulate the use of AI and ADM.

We suggest starting by considering whether the issues addressed in the principles may be fully or partly addressed in other areas of law, such as use of data and privacy, cyber security and information security, fair trading/competition law, consumer protection laws, anti-discrimination laws. Some principles and issues may be covered by multiple existing regimes. In these cases, we suggest the preferred approach is to revise existing regimes to reflect the government's AI and ADM policy, and/or to remove inconsistencies between existing legislation to reflect the government's AI and ADM policy. There are emerging differences between the Privacy Act, specific data regimes and the proposed digital identity legislation that may result in inconsistent data privacy protections while adding unintended friction to the user experience and the capacity to use data for new technologies. One example is the Privacy Act Review proposal to require data to be 'anonymised' rather than 'de-identified' before it is no longer protected by the Privacy Act. De-identification is well understood by industry and data technologists, while a new requirement to 'anonymise' data may cause confusion and lead to a greater aggregation of data, which may reduce the data's richness for the application of AI and ADM.

In other cases, regulations may be 'technology neutral' (that is, does not require the use of a manual or non-digital process), but drafted in a way that assumes a human interaction or decision-maker and thus impede the adoption of AI or ADM. In these cases, reviewing the legislation to make them neutral as to the use of technology would support the use of new technologies.

## **Consider case for regulatory response**

If the analysis identifies a clear gap in existing legislation, there may be a case to consider whether an additional response by Government or regulators may be warranted. Given the breadth of applications of AI and ADM, and the range of businesses that can use AI and ADM now and into the future, a range of regulatory and non-regulatory responses may be appropriate. For example, one response could be issuing guidance about applying the AI Ethics Principles issued by the Department of Industry rather than new legislation or regulations.

We also suggest the Government consider factors as the commercial and reputational incentives for a business to take a responsible approach to the use of AI or ADM; whether proposed regulation is fit for purpose to mitigate particular consumer detriment while retaining incentives to use AI to assist customers. Since many businesses are likely to procure AI and ADM services from a vendor, regulatory responses may also need to consider an Australian entity's bargaining power vis-à-vis their contractual counterparties.

Providing additional transparency about the use of AI and ADM can in itself be a step in building community confidence in these technologies. For example, more transparency about how the government will adhere to Australian and international best practices will help to build consumer confidence in this technology and can help to set the norms of AI and ADM use in the Australian economy more broadly.

## **Compliance with privacy law**

Government and the Office of the Australian Information Commissioner (**OAIC**) could consider providing further precedent or guidance to explore the nexus between privacy law and the adoption of AI or ADM. For reference, Norway's Data Protection Authority regulatory sandbox helps entities comply with AI-specific provisions of the EU General Data Protection Regulation (**GDPR**) and develop privacy-friendly AI solutions. Its aim is to produce helpful precedent for the most common use cases of AI and how they can comply with the trickier, more vague provisions of the GDPR (e.g. privacy by design). The approach relies on workshops and extended consultation between AI developers and regulators. The sandbox then delivers two deliverables: a detailed report on how organisations tweak or build their algorithms to comply with GDPR and their project plans. These are then communicated to the wider



community of organisations building AI. Something like this would help industry to understand best practice.

**ABA recommendations:** ABA recommends the Government:

- Identify and rationalise existing legislation so they are consistent with any Government principles on the use of AI.
- Review and amend legislation to be neutral as to whether a human or technology is used to make decisions or conduct a process.
- Give OAIC a clear mandate to provide guidance on how AI and ADM can be used in compliance with the Privacy Act.

## ‘Same risk, same rules’

Whether the Government proposes to take action to clarify existing law, introduce new principles or guidance, or consider new legislation, ABA advocates for a ‘same risk, same rules’ approach to any regulatory response.

While AI is used in regulated sectors such as telecoms and financial services, it equally has applications in businesses that are not subject to specific sectoral regulation. Requirements about the use of AI or ADM should apply consistently to economic activities that pose those risks, whether or not an activity is a regulated activity. Existing general legislation can be used to achieve this outcome instead of new, stand-alone legislation. For example, any principles, guidance or regulations about the use of ADM to make decisions about the provision of credit, or use of AI to steer a customer towards particular products or services, should apply to all entities that undertake this activity.

We consider this outcomes-based and risk-based approach would help to ensure Australia’s regulatory response remains broadly consistent with those of overseas jurisdictions.

**ABA recommendation:** the Government takes a ‘same risk, same rules’ approach to considering any regulatory response to AI and ADM.

## Consumer outcomes and vulnerability

ABA agrees with the Department of Industry’s ethical AI principles that AI should be fair, safe, reliable, transparent, contestable, human centred. Poor consumer outcomes that are linked to the use of AI and ADM – particularly outcomes that affect vulnerable consumers, can undermine public confidence in new technologies.

## Decision making in humans and technologies

Both human contact and AI/ADM have their particular characteristics, strengths and weaknesses. Each in their own way can produce or embed processes and decision-making frameworks that create good or poor consumer outcomes; human and technology-made decisions can both be biased or inconsistent. In each particular case, just as there may be unjustifiable variability in human-made decisions, a customer may receive a different outcome in a specific case when AI or ADM is applied – in some cases, the outcome may more accurately reflect the customer’s circumstances or the facts of the case.

We suggest any government policy that seeks to address quality of decision making and bias could hold the entities using AI or ADM to the same principles-based outcomes as for entities using human decision making. This may mean identifying a *pattern* of poor outcomes because biases have been coded into a model, or processes where the consumer is not provided adequate transparency and does not have the ability to escalate or challenge a decision (in other words, the use of AI/ADM should not produce a ‘black box’). This approach can help to promote good consumer outcomes while facilitating digital-first business models that predominantly use algorithmic decision making.

If the Government considers it would be desirable for businesses to be accountable for their use of AI and ADM or ways to provide transparency about the inputs to models, we reiterate the regulatory response should be appropriate to the problem identified. We also encourage the Government to



consider a range of options to achieve the outcome. For example, to support the quality of ADM, the Government could seek to provide access to data across industries (banks, accounting software providers, merchant providers, etc) to provide an “eyes wide open” approach when using automated decisions. We agree accountability or transparency policies should not require businesses to expose proprietary algorithms or IP.

### **Vulnerability**

The fact that customers may experience vulnerability and may benefit from extra care should not, in itself, be a reason to prohibit or limit use AI or ADM. On the other hand, at present, due to the cost, privacy impacts and data implications of using automation to respond to customers experiencing vulnerability, investment in humans rather than technological systems may often provide better care in a consistent, meaningful and timely way to customers experiencing vulnerability.

Bringing these perspectives together, businesses should be accountable for their use of AI or ADM. A company that uses AI or ADM should consider ways to mitigate the risk that the use of AI/ADM technology which may create less desirable or undesirable outcomes for customers, including vulnerable customers. A gap analysis will show to what extent this outcome can be achieved without new legislation. It makes more sense to leverage existing approaches to vulnerability where they already exist so that the issue of AI/ADM and vulnerability is part of any broader framework on vulnerability – for example the Banking Code of Practice which already contains provisions about vulnerability and extra care.