Australian Banking Association

14 August 2023

Technology Strategy Branch
Department of Industry, Science and Resources
GPO Box 2013
Canberra ACT 2601

Submitted via email: DigitalEconomy@industry.gov.au

ABA submission – safe and responsible use of AI

Summary

Banks have a history of using technology to improve customer service and enhance the security of banking. AI is already providing more tailored services and assistance to people, making some services more cost effective and/or accessible, improving the efficiency of some administrative or analytical work, and has potential to improve the consistency and quality of outcomes for consumers. Since AI is being used to target consumers in the commission of technology-enabled crimes, it is also important that banks and other legitimate actors can protect consumers by implement AI solutions which can better identify and address technology enabled crimes such as cybercrime and digital fraud.

The capabilities of AI technology are still developing. The range of activities and technologies which are understood to constitute 'AI' is also very broad and varied. Our understanding of the potential uses of AI and the impact of some uses, and what may be fit for purpose, governance of the development and use of AI, is also evolving.

ABA advocates for a considered and efficient approach by Government. Specifically:

- Consider whether further legislation is needed *after* mapping the application of existing law to aspects of this issue. If further legislation is considered necessary, also consider whether the legislation needs to apply to specific highly regulated sectors such as the banking sector;
- Consider using more flexible mechanisms such as regulator and industry guidance which can adapt as our understanding of this technology as it evolves. This includes ensuring coordination between government and regulatory agencies and facilitating alignment with international technical standards and appropriate regulatory responses;
- Find ways to provide clarity to businesses and users of AI and help both Australia and Australians to benefit from AI-enabled innovations and not fall behind other jurisdictions that Australia competes with for talent and investment;
- Consider the impact of prohibiting the use of AI if this inhibits the ability of Australian Government and businesses to protect themselves from malicious uses of AI;
- Further refine the risk-based framework set out in the consultation paper, including how the framework could consider the case for regulation that is proportionate to the type of risk and impact. The risk-based approach in the consultation paper only applies to use cases/users of AI but it should extend to AI developers and technology providers. A risk-based approach should also consider whether particular mitigants or remedies should be available; and
- Any banning of AI use cases should be considered on a case-by-case basis as a last resort.

Consider whether further legislation is needed

As the consultation paper acknowledges, the use of AI is subject to several existing laws. For example, the use of data to train a model must comply with existing laws relating to IP or privacy; and a model's outputs must comply with existing discrimination laws. For banks and financial service providers, the development or use of AI is also subject to specific legislation that provides strong consumer protections. In addition to existing legislation, banks have well established and sophisticated risk governance frameworks which consider many of the operational and technology risks that arise in non-AI contexts which equally apply in the implementation of AI tools.

ABA notes that regulators have taken strong and effective enforcement action in cases that involve the use of AI technology using existing, technology-neutral laws (e.g., the *Privacy Act 1988* (Cth)).

As a first step in its approach to determining suitable regulation for AI, Government should map potential concerns about AI against existing, relevant laws before deciding whether to introduce new legislation. Any further legislation or amendments should only be adopted:

- to address specific risks not already covered by existing regulatory regimes;
- to remove unintended or unnecessary impediments to realising potential and benefits; and
- on a risk- and principles-based approach which considers whether the legislation needs to apply to specific highly regulated sectors such as the banking sector;

More broadly, ABA supports any steps Government can take to, as much as possible, future proof all legislation by ensuring, amongst other things, due regard is had to the potential impact of such legislation on AI development and use in Australia. We note that further legislation would be complicated by the need to define the regulatory perimeter for ‘AI’.

Given the potential benefits of AI in banking and financial services, ABA supports the framing and application of financial services regulations in a way that is AI agnostic. This means that generally financial services regulation should apply irrespective of whether the regulated product or service is provided by a human, technology, or a hybrid. It also means if financial services regulation prevents or hinders use of AI in banking and financial services where there is no risk-based justification for that regulatory effect, ABA advocates for amending and removing these regulatory barriers.

Some potential harms that can result from the use of AI cannot be addressed by regulation; some require internationally coordinated action. The use of AI by cyber criminals, to commit scams and fraud (often by overseas criminal enterprises), or by malicious nation states are examples of such harm. As such, it is important to also consider scenarios where alternatives to legislation may provide a more appropriate response.

Consistency in Government and regulators’ approach

Irrespective of whether further legislation is adopted; it is critical for regulators to adopt a consistent approach to the development and use of AI. It is important for all organisations and businesses – those that develop the technologies and those that use them – to have clarity about regulatory requirements (and to whom they apply) and about the roles of agencies and regulators. Clarity about regulator roles and responsibilities is particularly important for highly regulated sectors like banking. Otherwise, industry will likely have to reconcile fragmented or conflicting approaches from different regulators as APRA, ASIC, AFCA, ACCC, OAIC, and others, under regulatory guidance or approach to supervision.

It is not necessary to adopt further regulations to achieve this objective. Alternatives include:

- Non-legislative mechanisms, such as a ‘hub and spoke’ model where a central agency or centre of excellence provides advice to agencies on how to consider AI outcomes in applying their specific legislation. Particular care should be taken to avoid inconsistencies between regulators.
- Industry best practice guidance for developers or users of AI. Guidance could relate to technical matters such as model development and documentation, governance, oversight and risk management frameworks for users and highlight examples of good and best practices.
- Government-industry / public-private collaboration using existing bodies like CSIRO to promote good practices such as voluntary ethical AI impact assessments, supported by voluntary certification; it can also provide funding for AI development and research.

- International coordination using both Government and private sector expertise. Specifically, ABA asks the Australian Government to engage with international standard-setting authorities (for example, government and/or regulators in Singapore, the UK and the US) and do so in coordination with industry (including organisations and sectors that are users of the technology).

Ways to address the development or use of AI under existing regulations include:

- Identify any gaps in the existing artefacts related to AI risks including AI unique risks. Consider how to address risks that already exist, while recognising the potential for AI to amplify some risks due to the scale and speed that action can be taken through the use of AI.
- Consider where AI-specific risks can be integrated into the existing frameworks without creating redundancy.
- Incorporate AI-related questions, guidelines, or criteria into the existing frameworks.
- Look for areas where existing assessment frameworks and risk management processes can be modified or expanded to include AI-specific and/or AI-related risks without creating separate and redundant processes.
- Remove or limit unintended or unnecessary regulatory impediments to AI, having regard to relevant risks and the potential prejudice to Australia, Australians, businesses and/or sectors.
- Continuously monitor and evaluate the effectiveness of the integrated approach.

One of the guiding objectives of any initiative should be promoting public and private sector investment in AI to ensure Australia can utilise its benefits and not fall behind other countries. Another objective could be promoting interoperability between Australian and overseas markets using specified international standards (ie, IOSCO guidance and ISO/IEC 23053:2022).

This approach would be broadly consistent with the UK white paper. The approach taken under the white paper is to leverage and build on existing regulatory regimes (e.g. privacy and product liability laws) and intervene in a proportionate and pro-innovation way to address regulatory uncertainty and gaps. The ABA is supportive of this approach.

Provide certainty and promote benefits of AI

The proposals made above can help to create a favourable environment for businesses and other organisations to adopt and use AI while ensuring appropriate consideration and mitigation of potential risks. Providing balanced information about the benefits of AI can promote acceptance by consumers and businesses and lead to faster adoption by Australia of new technology; the counterfactual could be that Australian businesses fall behind their regional or other international competitors, which can also affect our ability to attract or retain talent in research and academia.

Considering that AI can be used to both commit and combat criminal or malicious application of AI in cyber-attacks, fraud, and scams, adopting policies or initiatives that unduly inhibit the adoption and use of AI in Australia can also expose businesses and even government to these criminal and malicious actors who are generally not at all concerned about adhering to government controls or guidance unlike ABA members.

Fine-tune risk management approach

ABA in principle agrees with a risk-based approach to AI governance and oversight. As a society this means forming views about the extent to which individuals and businesses should be able to make decisions about how they engage with technology, whether and when there are public policy grounds to prohibit harmful practices, and (short of outright prohibitions) what other safeguards should be applied across the board or in specific circumstances. These decisions often involve trade-offs between various interests – for example, potential benefits of setting Australian-specific regulation as compared to the benefits of having a wider range of AI-enabled services and products available in Australia and at lower cost.

ABA advocates for an approach that is consistent with international standards, such as the US National Institute of Standards and Technology (NIST). NIST recently developed the AI Risk Management Framework to assist organisations to manage AI risks and promote the responsible development and use of AI systems.

In relation to the risk management approach set out in the consultation paper:

- A risk-based approach should set out a way to assess the types of risk that may relate to the developers, providers or users of AI, the impact of the risk, potential mitigants and residual risks.
- The proposed risk management approach considers impact but not types of risk.
- The risk management approach sets out controls for each level of impact. The controls and risk management frameworks that may be appropriate or necessary may depend on the type of risk or a particular use case, not (solely) on an assessment of impact. The requirement of having a human in loop may be appropriate in some cases, for other cases such as autonomous self-driving vehicles, a more appropriate consideration may be whether the vehicle can be used in urban vs agricultural settings (as well as human in loop). The proposals do not address the role of governance and risk management frameworks, or user education including for boards, executives and other senior leaders (including in government). Also see specific comments below on notices and disclosure of information.
- Sectoral regulation such as financial services regulation reflect existing, specific decisions about how particular risks (such as consumer protection or financial stability risks) should be managed, and to what extent these risks should be limited or avoided altogether. It is not clear how a general risk management approach would map onto existing regulatory regimes. For this reason in particular, ABA supports an approach which also recognises that there may need to be adjustments to regulations which have unintended and unnecessary limiting impacts on AI. Additionally, consideration should be given to the risk of overlap or duplication between regulation. One example is under the proposed privacy reforms, a proposal is included about automated decision making, which, if enacted alongside separate AI regulation might cause overlap or conflict.
- Query how a risk management approach may apply to the development of a model, as distinct from the application or use of a model.

ABA reiterates our view that a risk-based approach should be to identify AI-specific risks that is not addressed by existing legislation and regulations and consider the case for further regulation if there are AI specific risks or risks that are not adequately addressed under existing laws and regulations. If further legislation is considered necessary, also consider whether carve outs are appropriate for already-regulated sectors such as the banking sector to avoid duplication.

We believe the approach or initiatives proposed in earlier sections of the submission are consistent with a risk-based approach.

Notices and disclosure

Transparency is a useful governance principle in relation to the use of AI and technology. However, depending on the intended result of a notice or disclosure, a general requirement to provide information may not be useful or indeed adequate. Even where notices and disclosure are an appropriate control or mitigant, the actual effectiveness will depend on whether the content of information and the way in which it is provided is appropriate for the intended audience. For example:

- A general notice that a company is using AI to provide enhance customer service, or to enhance their cybersecurity or fraud monitoring, is unlikely to give a customer sufficient information to understand the implications for the customer of using the service or make an informed decision about whether to use a service. These notices can also give rise to notice fatigue, which can have the unintended consequence that the customer may also ignore specific warnings – such as a warning that a transaction could be fraudulent, and the customer should reconsider.

- Even the provision of fuller notices and system information, or providing information about how the AI makes decisions, may not help most users or customers to assess the potential risks of using a service. One example is where the onus lies with the entity deploying AI to avoid certain risks to physical safety altogether, rather than rely on a customer or employee to make a risk assessment based on system information.
- Publishing explanations about the output can be a commercially sensitive matter as it could require revealing the IP of the model.
- On the other hand, an explanation of output may not be meaningful to the end user or retail customer. In some cases, providing an explanation may not address the substantive issue of the user or customer wanting an avenue to seek a review of a decision or other recourse.
- What information is provided to experts or regulators also merit consideration. In applying principles-based legislation, it may be more appropriate for regulators to review whether an entity has governance and monitoring systems to ensure the entity's activities (including any output from a model) remain in compliance with applicable law, rather than to review code.

Rather than prescribing AI specific disclosures, another approach may be to consider how existing disclosures about decisions and outcomes – whether made by a human, AI, or a hybrid – are provided.

In more general terms, enhancing transparency from companies and Government about their policies or approach to using technology can enhance public confidence, especially if combined with other consumer-focused initiatives aimed at building awareness to help consumers to understand the information. Making general information available as an education or public confidence initiative should be encouraged, but not mandated, to provide more scope for these types of initiatives to evolve and reflect issues of interest or concern to the public. General information could address issues like:

- Roles, responsibilities, and accountability frameworks for AI and possibly governance of model development and validation;
- Data collection practices and use of data;
- In general terms, how algorithms may be used for decision-making.

Banning

Banning use of AI should be a measure that is used sparingly, considering the likely impact, effectiveness, and flow on consequences. Banning may not be effective where the actor using the technology is outside of Australia or is using technology for a criminal or malicious purpose. A ban on using a particular technology also means the same technology will not be available for purposes such as security and fraud prevention. Any decision to ban a use of technology should be based on expert advice and be targeted to specific use cases where outcomes have produced or inevitably will produce, harm that is disproportionate to benefit and which cannot be appropriately addressed or mitigated.

Yours Sincerely

Rhonda Luo

Policy Director