22 April 2022

BSA COMMENTS ON AUTOMATED DECISION MAKING AND ARTIFICIAL INTELLIGENCE REGULATION ISSUES PAPER

Submitted Electronically to the Digital Technology Taskforce

BSA | The Software Alliance (**BSA**)[1] welcomes the opportunity to provide comments to the Department of Prime Minister and Cabinet's Digital Technology Taskforce on its Issues Paper regarding automated decision making (**ADM**) and artificial intelligence (**AI**) regulation.[2]

BSA is the leading advocate for the global software industry before governments and in the international marketplace. Our members are at the forefront of software-enabled innovation that is fuelling global economic growth, including cloud computing and AI products and services. As leaders in AI development, BSA members have unique insights into both the tremendous potential that AI holds to address a variety of social challenges and the governmental policies that can best support the responsible use of AI and ensure continued innovation.

We welcome the Australian Government's recognition of the opportunities presented by the development and deployment of AI and ADM. These emerging technologies have the potential to generate substantial economic growth and enable governments to provide better and more responsive services, while addressing some of the most pressing societal challenges. However, a flexible policy framework is necessary to facilitate the responsible uptake of AI and ADM products and services.

Summary of BSA's Recommendations

- AI and ADM regulations should be: (1) informed by existing law, (2) risk-based, and (3) context-specific;
- Ensure international data transfers and open access to government data;
- Account for the different roles and responsibilities of stakeholders;
- Promote interoperability of regulations and standards; and
- Recommend tools and resources to help businesses mitigate risks of bias.

[1] BSA's members include: Adobe, Alteryx, Altium, Amazon Web Services, Atlassian, Autodesk, Aveva, Bentley Systems, Box, Cisco, CNC/Mastercam, Dassault, DocuSign, Dropbox, IBM, Informatica, Intel, MathWorks, Microsoft, Nikon, Okta, Oracle, PTC, Rockwell, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

[2] Issues Paper, "Positioning Australia as a leader in digital economy regulation – Automated Decision Making and AI Regulation", March 2022, https://www.pmc.gov.au/sites/default/files/automated-decision-making-ai-regulation-issues-paper.pdf

300 Beach Road
#30-06 The Concourse
Singapore 199555

P: +65 6292 2072
F: +65 6292 6369
W: bsa.org

Regional Representative Office
UEN: S97RF0005K

Recommendation 1: AI and ADM Regulations Should be Informed by Existing Law, Risk-Based, and Context-Specific

As the Australian Government considers AI and ADM regulations, we encourage the adoption of an approach that is: 1) informed by existing law, 2) risk-based, and 3) context-specific.

1) Informed by Existing Law

As the Issues Paper rightly notes, the development and use of AI are already subject to a wide range of existing legal protections and requirements**. Before considering new AI-specific laws or regulations, policymakers should first evaluate the adequacy of the existing legal framework to determine whether new regulations are needed and minimise regulatory duplication**. In evaluating the sufficiency of existing laws, policymakers should be guided by two considerations. First, to promote trust and confidence in AI, the public should be assured that the law will continue to afford the same level of protection irrespective of whether a decision is made by a person or an automated system. Second, to promote AI innovation and adoption, it is vital to ensure that there is sufficient clarity about how existing laws and regulations will apply to AI. **Based on the foregoing, we recommend that the Australian Government consider new AI and ADM regulations in circumstances where there is a demonstrated gap in the existing legal framework.** In addition, agencies and departments that oversee sector-specific regulations should examine existing legislation and guidelines — in consultation with the private sector — to determine whether the current rules are sufficient or require clarification regarding their application to AI.

2) Risk-Based

As a general principle, the scope of any regulatory obligations should be a function of the degree of risk and the potential scope and severity of harm. Many AI and ADM systems and the manner in which they are deployed pose extremely low, or even no, risk to individuals or society, and imposing onerous regulations on the entities developing and/or deploying such systems would only unduly hamper innovation. **Regulations should therefore focus on high-risk application of AI, such as uses of AI that may have a consequential impact on an individual's legal position (e.g., access to employment) or that pose a significant risk of physical harm.** To this end, it will be important to carefully assess scenarios that should be deemed as high-risk and hence be subject to legal requirements.

3) Context-Specific

The risks that AI poses and the appropriate mechanisms for mitigating those risks are largely context-specific. **Rather than regulating AI as a technology, regulatory activity should instead focus on particular applications of AI that may create specific risks**. Moreover, because the appropriate mechanisms for addressing risks will vary depending on the nature of the AI system and the setting in which it is being deployed, regulators should avoid prescriptive, one-size-fits-all technical requirements. Instead, BSA encourages regulatory approaches that provide incentives to adopt process-based accountability mechanisms, such as impact assessments, for particularly high-risk applications of AI.

Recommendation 2: Ensure International Data Transfers and Open Access to Government Data

AI and ADM systems are "trained" by ingesting enormous volumes of data. Their benefits are therefore dependent on the quantity and quality of data that is available for training. As a result, government policies affecting the ability to access and share data have a significant influence on the development of AI and ADM, and the quality of their outcomes. **To promote innovation and adoption of AI and ADM, the Government should: 1) ensure that data may be transferred**

across borders; and 2) support an open government data policy to make non-sensitive government data assets freely available and useable for the general public.

1) Ensure international data transfers are unimpeded

International data transfers are integral to every stage of the AI life cycle, from the development of predictive models to the deployment and use of AI and ADM systems. Data used in these systems often originate from many geographically dispersed sources. Many AI and ADM solutions used in Australia are developed internationally and offered over cloud computing systems. Likewise, AI and ADM solutions developed in Australia rely on international data transfers both for their development and deployment.

In this regard, we are encouraged that Australia's Digital Trade Strategy[3] expressly acknowledges the importance of facilitating cross-border data transfers and prohibiting data localisation requirements. As the Digital Trade Strategy notes, "[u]nnecessary restriction on the flow of data, or requirements to store data locally raises costs for businesses and significantly reduces efficiencies, impacts the ability to make decisions on business development, marketing, innovation and development of comparative advantage, and makes it difficult for businesses to enter new markets".[4] This policy position aligns with both the Singapore-Australia Digital Economy Agreement[5] and the Australia-United Kingdom Free Trade Agreement's Digital Trade Chapter,[6] which contain binding rules on cross-border data transfers and prohibitions on data localisation.

To ensure that Australians benefits from continued AI and ADM innovation, BSA encourages the Australian Government to prioritise implementation of the Digital Trade Strategy.

2) Access to government data and public sector information

BSA supports an open data policy through which non-sensitive government data should be made open, available, and useable for the general public. Government-generated data is a resource that can serve as a powerful engine for creating new jobs and promoting economic growth. At both the local and national level, governments collect and generate vast quantities of non-sensitive data that can be harnessed in the development of AI and ADM systems. For instance, an AI system designed to improve supply chain efficiency can leverage government data about historical traffic flows, law enforcement event advisories, and weather patterns to recommend delivery routes that minimise congestion, reduce emissions, and improve public safety.

While the recently legislated *Data Availability and Transparency Act 2022* (**DAT Act**) is a step in the right direction, it represents a missed opportunity to expand access to government data in Australia for the aforementioned purposes in the near-term. Under the current DAT Act, the Australian Government may only share government data with "accredited users" for specific purposes (e.g., delivery of government services, informing government policies and programs, and research and development). Foreign entities are not able to become accredited users under the DAT Act's accreditation scheme, which means that "government data may not be shared with a foreign entity".[7]

---

[3] Digital Trade Strategy, April 2022, https://www.dfat.gov.au/sites/default/files/digital-trade-strategy.pdf.

[4] Digital Trade Strategy (2022), p. 10.

[5] Singapore-Australia Digital Economy Agreement, https://www.dfat.gov.au/sites/default/files/australia-singapore-digital-economy-agreement.pdf, Articles 23-25.

[6] Australia-United Kingdom Free Trade Agreement, Digital Trade Chapter, https://www.dfat.gov.au/trade/agreements/not-yet-in-force/aukfta/official-text/australia-uk-fta-chapter-14-digital-trade, Articles 14.10-14.11.

[7] Revised Explanatory Memorandum, Data Availability and Transparency Bill 2022, March 2022, https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r6649_ems_452a2c9f-210a-4497-8c07-6a336ec6e0d0/upload_pdf/Data%20Availability%20and%20Transparency%20Bill%20%20-%20Revised%20EM.pdf;fileType=application%2Fpdf, para 10.

The DAT Act also currently precludes businesses from participating in the accreditation scheme "to provide an opportunity for the Scheme to establish and mature".[8] As such, AI developers do not have at their disposal easy access to Australian Government datasets which may be used to train AI and ADM systems, reducing the opportunities for innovation.

BSA encourages the Australian Government to ease the above restrictions during subsequent reviews of the scheme[9] to facilitate access to and use of non-sensitive government data to support domestic innovation and development in AI and ADM.

Recommendation 3: Account for the Different Roles and Responsibilities of Stakeholders

To the extent new AI and ADM regulation is contemplated, it should account for the unique roles and capabilities of the entities that may be involved in an AI system's supply chain. To that end, **regulatory obligations (and associated liabilities) should fall on the entity that is best positioned to both identify and efficiently mitigate the risk of harm that gave rise to the need for the regulation.**[10]

Reflecting the inherently dynamic nature of AI systems, AI and ADM regulations must account for the array of stakeholders that may play a role in various aspects of a system's design, development, and deployment. In general, there are at least two key stakeholders with varying degrees of responsibility for managing the risks associated with an AI system throughout its lifecycle:

- **AI Developers:** AI Developers are organisations responsible for the design and development of AI systems.

- **AI Deployers:** AI Deployers are the organisations that adopt and use AI systems — if an entity develops its own system, it is both the AI Developer and the AI Deployer.

The appropriate allocation of risk management responsibilities between such stakeholders will vary depending on the nature of the AI system being developed and which party determines the purposes and means by which the underlying model is trained. For instance:

- **Universal Model:** The term "universal model" is used to describe circumstances in which an AI developer provides multiple customers (i.e., AI deployers/users) with access to a single pretrained model.
    - In circumstances involving a Universal Model, the AI developer will bear responsibility for most aspects of risk management as the model is being designed and developed. Following deployment, risk management functions may be shared between the Developer and the Deployer of the system.

[8] Revised Explanatory Memorandum (2022), para 11.

[9] Revised Explanatory Memorandum, para 32, states: "To ensure the Scheme remains relevant and adaptable to evolving technology and public expectations, the Bill provides for an independent review three years after the Scheme's commencement. This is in addition to a review three months after the commencement of any amendments to the Privacy Act that would have a material impact on the Scheme."

[10] The importance of such an approach to AI regulation is a key pillar of the Organisation for Economic Co-operation and Development's (**OECD's**) Recommendation of the Council on Artificial Intelligence, which recognises that effective AI policies must account for "stakeholders according to their role and the context" in which AI is being deployed. *See* Recommendation of the Council on Artificial Intelligence, May 2019, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449. Per the Recommendation, the AI stakeholder community "encompasses all organizations and individuals involved in, or affected by, AI systems, directly or indirectly."

- **Customisable Model:** The term "customisable model" is used to describe circumstances in which an AI Developer provides a pre-trained model for AI Deployers that can customise and/or retrain the model using their own data.
    - While the AI Developer will be responsible for risk management of design decisions, risk management associated with the development and deployment stages will be a shared responsibility between the AI Developer and the AI Deployer.

- **Bespoke Model:** The term "bespoke model" is used to describe circumstances in which the AI Developer trains a bespoke AI model on behalf of an AI Deployer using the AI Deployer's data.
    - In instances involving a Bespoke Model, the AI Deployer will bear the bulk of risk management obligations.[11]

To that end, it is critical that AI and ADM regulations account for the unique roles and responsibilities of *developers* of AI systems and the organisations that *deploy* such systems. In many instances — especially those involving general-purpose AI tools — developers will not be in a position to know the precise manner in which the technology is being deployed. In such circumstances, the party best positioned to address potential risks will be the entity that deploys an AI system and determines the purposes and means by which it is used. Including such a conceptual distinction would be helpful to different stakeholders as they carry out risk assessments to determine the appropriate measures to adopt for AI development, deployment, and use. Of course, in many instances, particularly in the context of B2B arrangements, obligations for risk management will be most efficiently allocated through contractual agreement. Accordingly, any legislative framework should provide flexibility to enable organizations to negotiate terms that are tailored to the unique considerations of the B2B transaction that they are contemplating.

Relating to our Recommendation 1 above, it is also important to carefully assess the scenarios where the use of AI and ADM systems would be deemed "high-risk" and thus subject to legal requirements. Stakeholder involvement is crucial in this context, as this assessment will be both sector and use-case dependent. As such, **BSA recommends ensuring that clear language for broad stakeholder involvement[12] is included in any future regulation,** to promote a beneficial interaction between developers — which may not have extensive experience or presence in a specific sector that may be deemed high-risk — and deployers. **We also urge the Government to continually engage with stakeholders throughout the regulatory process, and *especially* in the implementation and enforcement phase.**

Recommendation 4: Promote Interoperability of Regulations and Standards

Australian leadership in the development and use of AI will be possible only if Australian companies can access global markets. To ensure Australian innovation can thrive in foreign markets, **it will be vital to ensure that the Australian approach to AI and ADM regulation is interoperable with global partners**. The Organisation for Economic Cooperation and Development's (**OECD's**) Recommendation represents an important first step toward establishing global norms around the governance and regulation of AI. Those norms are predicated on a risk management-based approach for enhancing the benefits of AI and safeguarding against unintended harms. Future Australian regulation should seek to align with OECD's guiding principles. It is encouraging that Australia's own

[11] The OECD for the Classification of AI Systems adopts a similar approach for assigning risk management responsibilities. See OECD Framework for the Classification of AI Systems, February 2022, https://www.oecd-ilibrary.org/docserver/cb6d9eca-en.pdf?expires=1649808351&id=id&accname=guest&checksum=74B738F154B4F05D18B7B3D8B3477CE0, p. 48.

[12] Per the Recommendation, the AI stakeholder community "encompasses all organizations and individuals involved in, or affected by, AI systems, directly or indirectly."

AI Ethics Framework[13] was developed with reference to existing initiatives, including the OECD's Recommendation and the European Union's Ethics Guidelines for Trustworthy AI.[14] There are also various efforts underway to establish internationally recognised standards for AI, including within the International Organisation for Standardization (**ISO**) and the Institute of Electrical and Electronics Engineers (**IEEE**).[15] **BSA urges that, in designing regulations and adopting standards for AI and ADM, the Government should continue to align them with global norms and strive to make them interoperable with other jurisdictions.**

Recommendation 5: Recommend Tools and Resources to Help Businesses Mitigate Risks of Bias

The Issues Paper identifies the potential for bias or discrimination as "a significant issue for the designers of systems implementing AI and ADM".[16] In recognition of such concerns, BSA recently published *Confronting Bias: BSA's Framework to Build Trust in AI* (BSA Framework).[17] The BSA Framework is a first-of-its-kind methodology that organisations can use to perform impact assessments to identify and mitigate risks of bias that may emerge throughout an AI system's lifecycle. The BSA Framework:

- Outlines a process for performing impact assessments to identify and mitigate potential risks of bias;
- Identifies existing best practices, technical tools, and resources for mitigating specific AI bias risks that can emerge throughout an AI system's lifecycle; and
- Sets out key corporate governance structures, processes, and safeguards that are needed to implement and support an effective AI risk management program.

BSA encourages the Government to leverage the research and best practices in the BSA Framework to create relevant guiding materials for businesses around how they can mitigate bias in AI and ADM development and deployment/use.

Conclusion

We hope that our comments will assist the Government as it considers regulations for AI and ADM in Australia. Please do not hesitate to contact me if you have any questions regarding this submission or if I can be of further assistance.

Sincerely,

Tham Shen Hong
Manager, Policy – APAC

---

[13] Artificial Intelligence Ethics Framework, November 2019, https://www.industry.gov.au/data-and-publications/australias-artificial-intelligence-ethics-framework

[14] Developing the AI Ethics Framework and principles, https://www.industry.gov.au/data-and-publications/australias-artificial-intelligence-ethics-framework

[15] See: https://www.iso.org/committee/6794475.html and https://standards.ieee.org/initiatives/artificial-intelligence-systems/.

[16] Issues Paper (2022), p. 10.

[17] Confronting Bias: BSA's Framework to Build Trust in AI, June 2021, https://ai.bsa.org/wp-content/uploads/2021/06/2021bsaaibias.pdf. A summary of BSA's framework is appended to this submission.

The Software Alliance

BSA

Confronting Bias: BSA's Framework to Build Trust in AI

Tremendous advances in artificial intelligence (AI) are quickly transforming expectations about how the technology may reshape the world and prompting important conversations about equity. While AI can be a force for good, there is a growing recognition that it can also perpetuate (or even exacerbate) existing social biases in ways that may systematically disadvantage members of historically marginalized communities. As AI is integrated into business processes that can have enormous impacts on people's lives, there is a critical need to ensure that organizations are designing and deploying these systems in ways that account for the potential risks of unintended bias.

The Framework is a tool for ensuring that AI is accountable by design and can be used by organizations of all types to manage the risk of bias throughout a system's lifecycle. Built on a vast body of research and informed by the experience of leading AI developers, the Framework:

Outlines a process for performing impact assessments to identify and mitigate potential risks of bias

Identifies existing best practices, technical tools, and resources for mitigating specific AI bias risks that can emerge throughout an AI system's lifecycle

Sets out key corporate governance structures, processes, and safeguards that are needed to implement and support an effective AI risk management program

The Framework is a playbook organizations can use to enhance trust in their AI systems through risk management processes that promote fairness, transparency, and accountability. It can be leveraged by organizations that develop AI systems and companies that acquire and deploy such systems as the basis for:

- **Internal Process Guidance.** The Framework can be used as a tool for organizing and establishing roles, responsibilities, and expectations for internal risk management processes.
- **Training, Awareness, and Education.** The Framework can be used to build internal training and education programs for employees involved in developing and using AI systems, and for educating executives about the organization's approach to managing AI bias risks.
- **Supply Chain Assurance and Accountability.** AI developers and organizations that deploy AI systems can use the Framework as a basis for communicating and coordinating about their respective roles and responsibilities for managing AI risks throughout a system's lifecycle.
- **Trust and Confidence.** The Framework can help organizations communicate information about a product's features and its approach to mitigating AI bias risks to a public audience. In that sense, the Framework can help organizations communicate to the public about their commitment to building ethical AI systems.
- **Incident Response.** Following an unexpected incident, the processes and documentation set forth in the Framework can serve as an audit trail that can help organizations quickly diagnose and remediate potential problems.

To download the full report visit www.bsa.org