Australian Information
Industry Association

Australian Information Industry Association

Submission on

Use of Automated Decision-Making by Government Consultation Paper

Introduction

The Australian Information Industry Association ('AIIA') appreciates the opportunity to provide feedback to the Attorney General's Department ('AGD') on the use of automated decision-making ('ADM') by government.

ADM and AI offer enormous potential to boost efficiency and accuracy in public services. However, as starkly illustrated by the Robodebt Royal Commission, poorly managed ADM can undermine public trust. This consultation is a critical chance to address Recommendations 17.1 and 17.2 of the Royal Commission into the Robodebt Scheme ('Robodebt Report')[1] by establishing clear legal frameworks, improving transparency, and strengthening oversight.

For these reasons, the AIIA is keen to support the government to become an exemplar user of ADM and AI. Our submission stresses the necessity for explicit distinctions and robust frameworks regulating ADM and AI. It advocates for ethically deployed and transparent ADM systems to ensure public trust. Recommendations include maintaining clear separation between ADM and AI, implementing risk-based criteria, and establishing standardised safeguards and oversight. The submission highlights the importance of protecting sensitive information while enhancing public accountability and compliance through structured transparency and regular audits.

Defining and Distinguishing between ADM and AI

ADM and AI are distinct yet interconnected technologies. ADM involves the use of algorithms or predefined rules to execute tasks without adaptive changes, functioning within a set framework. Conversely, AI mimics human cognition and reasoning, capable of learning from data and making decisions in complex scenarios. It is crucial for frameworks to clearly distinguish between ADM's fixed-rule operations and AI's adaptive learning capabilities to avoid conflation, 'scope creep', and ensure effective governance.

Object of Government being an Exemplar in Using ADM and AI

The AIIA is encouraged by the AGD's balanced overview of the benefits and risks of ADM. This demonstrates that the AGD understands the value of ADM across a range of public sector contexts, while acknowledging legitimate risks.

As one of the largest adopters of ADM systems, government agencies are uniquely positioned to set benchmarks for best practices, ethical deployment, and transparency in ADM. Importantly, safeguards around government use of ADM are paramount because they affect a decision around the citizen. More importantly, citizens are especially vulnerable or beholden to the specific government agency for the service due to the lack of alternative service providers. By prioritising clarity in communication, embedding fairness into system

[1] Royal Commission into the Robodebt Scheme, Report of the Royal Commission into the Robodebt Scheme (Commonwealth of Australia, 2023).

design, and fostering an environment of ongoing evaluation and improvement, government agencies can serve as exemplars for responsible ADM adoption.

The AIIA notes the government's role is not only in regulating AI technologies but also in enabling innovation through leadership and fostering trust in automated systems. Public trust in ADM technologies will not stem solely from regulations—it will depend on the government's ability to showcase tangible benefits, address risks proactively, and model best practices in its own use of automation. The government can not only ensure that ADM systems serve the public interest but also lay the foundation for broader adoption of innovative technologies across sectors, positioning Australia as a leader in responsible and effective ADM governance.

Interaction with Other Government Reforms

We support the AGD's ambition to align the ADM framework with AI mandatory guardrails, where appropriate. This alignment ensures that both frameworks reinforce each other. This will, in turn, improve mutual understanding and compliance for improved government service delivery.

Balancing Transparency and Protection of Sensitive Information

Transparency is a cornerstone of trust in ADM systems, especially when deployed by government agencies. It ensures public accountability, fosters trust, and allows individuals to understand how decisions that impact their lives are made. However, transparency must be carefully balanced against the need to protect sensitive information, including intellectual property, commercially sensitive data, and national security interests.

The Consultation Paper highlights the challenges of balancing transparency with confidentiality, particularly in the context of algorithmic processes that may be difficult for the public to interpret. It is important to distinguish between transparency of outcomes, processes, and principles, and transparency of the underlying algorithmic models or source code.

A tiered approach to transparency should guide this balance. Agencies should publish plain-language summaries of ADM principles, objectives, and safeguards, as well as illustrative case studies demonstrating system functionality. Such plain language explanations will better serve citizens in understanding the underlying considerations and consistency of processes and in challenging decisions made.

Our main concern with this section is the proposal to directly *publish* business rules and algorithms. This could present risks around IP theft and security fraud. Complex algorithms are also likely to be misinterpreted. For this reason, detailed technical and algorithmic information should remain restricted to oversight bodies, with exemptions appropriately applied for national security, trade secrets, and operational risks. Exemptions should be reviewed periodically to ensure they remain justified and proportionate to the risks

involved. Furthermore, rather than a requirement to publish algorithms, AGD's goal could instead be achieved through auditing/compliance mechanisms, as outlined in the section on system-level safeguards.

To ensure consistency across government agencies, transparency requirements must be standardised under a centralised reporting framework. Agencies could consider adhering to minimum standards, including:

- Notification to individuals when ADM is used in decisions that affect them.
- Public disclosure of the general methodologies, principles, and safeguards underpinning ADM systems.
- Annual reporting on key ADM performance metrics, including error rates, decision volumes, and identified risks.

These standards are consistent with the principles outlined in the Automated Decision-Making Better Practice Guide[2], which emphasises that '[t]he underlying…rules of an automated system must be readily understandable and information about automated systems should be publicly available.'[3] Centralised reporting guidelines will ensure transparency obligations are consistently applied across agencies and facilitate meaningful comparisons and oversight.

It is also essential to balance transparency requirements with the risk of "notification fatigue." Overly frequent or poorly targeted notifications may reduce public understanding and trust rather than enhance it. Flexibility should be embedded into notification requirements, allowing agencies to tailor approaches based on the risk profile and nature of ADM applications.

Notification Requirements

Effective notification is a cornerstone of transparency in ADM systems, ensuring individuals understand when and how these systems are used in decisions that affect them. This notification should occur both before the application process and at the time of decision communication, especially for high-stakes decisions, to ensure individuals are adequately informed. However, agencies should have discretion to tailor notification timing based on the risk profile and operational requirements of specific ADM systems.

Part 15 of the recently enacted Privacy and Other Legislation Amendment Bill[4] has greatly increased the transparency requirements for organisations that implement ADM systems to make decisions significantly affecting individuals' rights or interests, consistent with proposals 19.1 and 19.2 of the Privacy Act Review Report[5]. Global precedents have also

[2] Commonwealth Ombudsman, Automated Decision-Making Better Practice Guide (2021).
[3] Ibid 25.
[4] Privacy and Other Legislation Amendment Bill 2024 (Cth).
[5] Department of the Attorney-General, *Privacy Act Review Report* (2023).

highlighted the importance of notification requirements, which is presumed in Article 22 of the GDPR[6] as a prerequisite for individuals to exercise their right to object, along with Articles 13(2)(f), 14(2)(g) and 15(1)(h) explicitly including notification of the existence of ADM in the list of further information that is required to be disclosed. This principle is reinforced in the *Guiding Principles for Automated Decision-Making in the EU*, which states '[d]isclosing the fact that the system is automated…would allow parties to make informed decisions, minimise the manipulative or misleading effects of such a system, and enable objections to be subjected to such automated processes, where applicable.'[7]

Safeguards Across the ADM Lifecycle

The implementation of ADM systems must be guided by safeguards spanning the entire lifecycle, from pre-implementation design and risk assessment to system-level performance monitoring, individual decision safeguards, and post-decision review rights.

Pre-Implementation Safeguards

The design and deployment of ADM systems must be underpinned by robust pre-implementation safeguards. Agencies must undertake comprehensive risk assessments before ADM systems are introduced, with a focus on human rights impacts, privacy and data security considerations, and compliance with administrative law principles, including procedural fairness and natural justice. These risk assessments should not be conducted in isolation but must involve cross-disciplinary collaboration. Experience from Canada shows there can be a high degree of inconsistency in how risk assessments are conducted across different agencies and use cases. AGD could consider establishing centralised/standardised guidance to support agencies in understanding risks and mitigation options.

Legal, technical, and policy experts must work together to evaluate risks and ensure ADM systems are aligned with legislative and ethical standards. Additionally, pilot testing should be mandatory for all high-risk ADM systems. Controlled trials will enable agencies to identify biases, coding errors, and operational inconsistencies before full-scale deployment.

System-Level Safeguards

At the system level, continuous monitoring and auditing are essential to maintaining ADM integrity and compliance. Agencies should implement mechanisms for regular internal and external audits, supported by robust record-keeping practices. These audits should assess system accuracy, identify emerging risks, and verify alignment with evolving legislative and policy frameworks. ADM systems must also remain dynamic and adaptable. Legislative and policy changes should trigger system updates, ensuring ongoing alignment with regulatory obligations. It's important that agencies also have incident response processes in place to respond to malicious actors that may seek to subvert ADM systems for personal gain.

[6] General Data Protection Regulation (EU) 2016/679.
[7] European Law Institute, Guiding Principles for Automated Decision-Making in the EU (Report, May 2022) Principle 4.

Decision-Level Safeguards

At the level of individual decision-making, ADM systems must incorporate safeguards to prevent errors and ensure fairness. Decision pathways must allow humans to intervene, particularly in cases involving ambiguity, high-risk outcomes, or significant impacts on individual rights. Decision-makers should have the authority to substitute or override incorrect ADM decisions when errors are detected. Human intervention was outlined in the Robodebt Report as one of the most effective safeguards to prevent system failure and preserve accountability[8], in addition to being included in the proposed Mandatory Guardrails for AI in High-Risk Settings.[9]

Equally important is the provision of clear explanations to affected individuals. Agencies must ensure that ADM decisions are accompanied by accessible explanations, detailing the factors considered and the reasoning behind the outcomes. This transparency supports trust and facilitates informed appeals where necessary.

Notwithstanding, we reiterate the importance of taking a risk-based approach. While pathways for human referral and oversight are appropriate, this won't be able to be achieved as a blanket requirement - the level and scope of human oversight will need to be tailored to the use case and level of risk. This aligns with the principles outlined in the AIIA's submission on Proposals for Mandatory Guardrails for High-Risk AI Settings, which emphasises that safeguards and oversight mechanisms should be proportionate to the potential harm posed by a system.

Post-Decision Safeguards and Merit Review Rights

In the post-decision phase, it is critical to ensure that individuals affected by decisions made by ADM systems have a clear path for review. The Robodebt Report emphasises the importance of review pathways[10], aligning with international AI standards.[11] [12] The AIIA recommends that both internal and external review mechanisms are made available, with independent bodies overseeing appeals to ensure impartiality and fairness. Additionally, agencies must have mechanisms to address identified errors swiftly, including the retroactive correction of decisions to minimise harm.

Exemptions to ADM safeguards must be tightly controlled and reserved for scenarios involving national security, law enforcement, or low-risk administrative processes with minimal impact on individual rights. These exemptions should be subject to periodic review to ensure they remain appropriate and proportionate.

---

[8] Royal Commission into the Robodebt Scheme, Report of the Royal Commission into the Robodebt Scheme (Commonwealth of Australia, 2023) 487.

[9] Guardrail 5, Department of Industry, Science and Resources, Safe and Responsible AI in Australia: Proposals paper for introducing mandatory guardrails for AI in high-risk settings (5 September 2024) 37.

[10] Royal Commission into the Robodebt Scheme (Final Report, July 2024) vol 2, 486.

[11] General Data Protection Regulation (EU) 2016/679, art 22(3).

[12] OECD, OECD Principles on Artificial Intelligence (OECD Legal Instruments, 2019) Principle 1.3.

Summary of recommendations

The AIIA again thanks the Department for the opportunity to provide insights and input on behalf of the ICT industry. For easy of reference, we have summarised our recommendations below:

1. **Definition and Scope**
- Maintain clear distinction between ADM and AI systems
- Apply risk-based criteria for regulating ADM use in decisions and administrative actions
- Exclude low risk use cases from full framework requirements

2. **Transparency and Protection:**
- Maintain clear notification requirements
- Implement alternative compliance mechanisms instead of publishing algorithms
- Protect intellectual property and security considerations

3. **Implementation Safeguards:**
- Develop centralised risk assessment guidance
- Establish standardised risk assessment procedures
- Create incident response protocols for system subversion

4. **Oversight and Review:**
- Implement risk-appropriate human oversight
- Establish auditing frameworks for oversight
- Ensure robust merit review rights

5. **Monitoring and Reporting:**
- Create standardised monitoring frameworks
- Establish clear incident reporting procedures
- Implement regular system audits

Conclusion

The AIIA appreciates the opportunity to contribute to this consultation and recognises the significant potential of automated decision-making systems to enhance government efficiency and service delivery. We note that the use of ADM by government is long standing practice; for example, s 6A of the *Social Security (Administration) Act 1999* was inserted into that Act nearly 25 years ago in 2001 so the 'Secretary may arrange for use of computer programs to make decisions'. However, their continued effective implementation requires robust safeguards, clear accountability mechanisms, and a balanced approach to transparency to maintain public trust and ensure fair and reliable outcomes.

Should you require further information, please contact Ms Siew Lee Seow, General Manager, Policy and Media, at siewlee@aiia.com.au or 0435 620 406, or Mr David Makaryan, Advisor, Policy and Media, at david@aiia.com.au.

Thank you for considering our submission.

Yours sincerely

Simon Bush
CEO, AIIA

About the AIIA

The AIIA is Australia's peak representative body and advocacy group for those in the digital ecosystem. Since 1978, the AIIA has pursued activities to stimulate and grow the digital ecosystem, to create a favourable business environment for our members and to contribute to Australia's economic prosperity. We are a not-for-profit organisation to benefit members, which represents around 90% of the over one million employed in the technology sector in Australia. We are unique in that we represent the diversity of the technology ecosystem from small and medium businesses, start-ups, universities, and digital incubators through to large Australian companies, multinational software and hardware companies, data centres, telecommunications companies and technology consulting companies