Submission to the Department of Industry, Science and Resources:

Safe and responsible AI in Australia

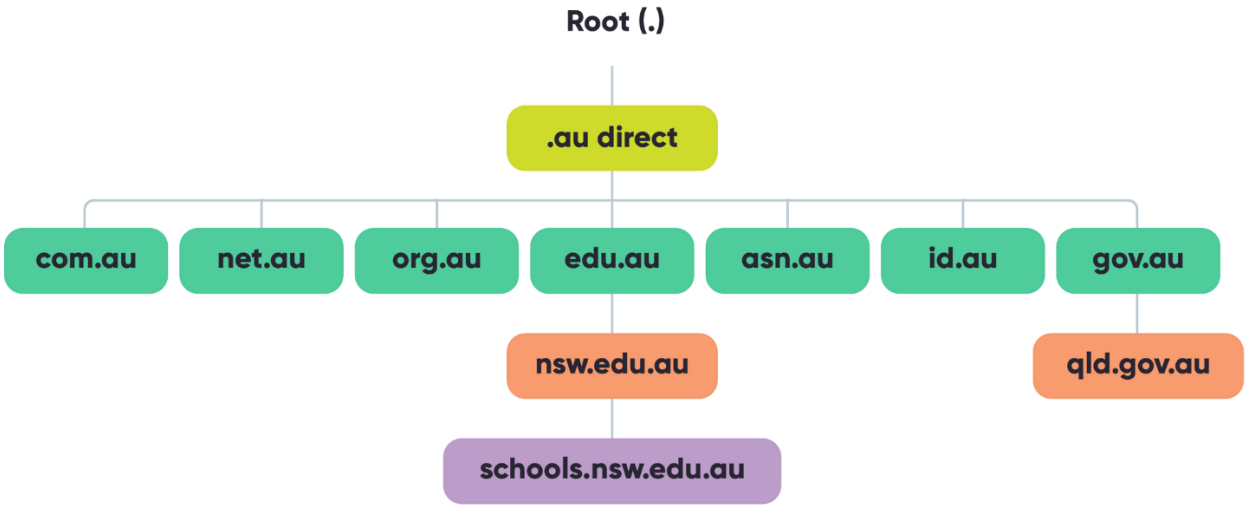
July 2023

.auDA

Table of Contents

About auDA

.au Domain Administration Limited ("auDA") is the trusted administrator of the .au country code Top Level Domain (ccTLD). The .au ccTLD includes the following namespaces:



The .au ccTLD is part of Australia's critical infrastructure, supporting more than 4 million .au domain names. auDA is a not-for-profit, endorsed by the Commonwealth Government to ensure it is a secure, accessible and trusted Australian public asset for all Internet users.

In performing its functions, auDA operates under a multi-stakeholder model, working closely with suppliers, business users, industry, civil society, consumers and the Australian Government. It seeks to serve the interests of the internet community as a whole and takes a multi-stakeholder approach to internet governance, where all interested parties can have their say.

To find out more about auDA, visit www.auda.org.au.

Submission

Executive summary

The governance[1] of artificial intelligence (AI) is an important topic of public discussion nationally and internationally. auDA believes that the policy framework should be shaped to emphasise the importance of utilising the technology for good. This requires policymakers and regulators to adopt a human-centric approach towards innovation to unlock positive economic and social value for all Australians.[2]

It is through this lens that auDA makes the following key suggestions:

- aligning terminology and definitions with those agreed upon and used by likeminded jurisdictions to develop an internationally harmonised approach towards AI governance
- establishing a multi-regulator sandbox facilitated through a multi-stakeholder approach to ensure inclusive policy design and a more balanced ecosystem for AI innovation
- imposing bans on AI applications that pose unacceptable risks to Australians, their fundamental rights and digital wellbeing
- enhancing education and awareness-raising efforts to support Australians across all ages and backgrounds in developing understanding of and trust in AI
- adopting a non-regulatory proportionate risk-based approach towards AI governance that maximises economic and social benefits, and minimises harms
- assessing cyber security implications of AI systems and how to protect Australians from AI-enabled scams and cyber threats

Below, auDA provides detailed comment on select questions raised in the Discussion Paper and on other areas auDA considers relevant.

[1] The Discussions Paper uses the term 'governance' to include the regulatory and voluntary mechanisms. According to the Discussion Paper (see p. 4) these mechanisms can include regulations, standards, tools, frameworks, principles and business practices.

[2] Digital technologies including AI and their implications for the Australian economy and society form an integral part of auDA's Public Policy Agenda, which sets out the issues central to our policy and advocacy activity during 2023-24. Through our contributions to relevant policy debates and developments, auDA intends to help foster an empowering and secure digital environment that puts people first.

Response to select discussion paper questions

Definition of AI (Q1)

The Department uses multiple different definitions proposed by the International Standards Organization (ISO), Commonwealth Ombudsman, and academia to describe and define AI and related systems, applications and functions including machine learning, automated decision-making, generative AI, multimodal foundational models, large language models, and algorithms.

The use of this terminology and related definitions from various sources differs from those already agreed upon and adopted by intergovernmental organisations and likeminded trading partners in their non-regulatory approaches or legislative frameworks addressing AI, including for example:

- In the *Proposal for a Regulation of the European Parliament and of the Council – Laying Down Harmonised Rules on Artificial Intelligence (AI Act) and Amending Certain Union Legislative Acts*, the European Union (EU) defines AI-related terms including "artificial intelligence system"[3] and different AI techniques and approaches including "machine learning approaches", "logic- and knowledge-based approaches", and "statistical approaches"[4].
- The *US Blueprint for an AI Bill of Rights* uses the umbrella term "automated system" to capture a multitude of terms including "system, software, or process".
- The OECD.AI has developed a Framework for Classifying AI systems based on the type of model used, data and input, output, economic context, and impact on humans, converging with the themes identified in this Discussion Paper. Some of the concepts outlined in the OECD definition are also reflected in the EU AI Act.
- The definition of "AI systems" proposed by the Government of Canada in its *Artificial Intelligence and Data Act (AIDA)*, published as part of *Bill C-27*, also aligns with concepts developed by the OECD.

Deploying terminology and definitions that are internationally compatible helps to minimise differences in the understanding of the technology, and to optimally address the risks and threats posed by the technology. This is of relevance when moving forward to develop harmonised frameworks, standards and potentially rules (see also our response to **Q4**).

[3] See Article 3(1) in EU AI Act.
[4] See also Annex I, available at: https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_2&format=PDF (accessed on 10 July 2023).

Coordination of AI governance across government (Q4)

In auDA's view, cross-government coordination should provide the foundation for a whole-of-government approach towards digital economy policy.[5] Cross-government coordination helps avoid repetitive consultation processes and duplication and fragmentation of regulation and reduce uncertainty and unintended consequences.

With respect to AI governance, auDA believes that establishing mechanisms for interagency collaboration and coordination to ensure that AI governance tools are consistent and complementary across different government entities should be a preferable approach. Given the omnipresence of AI in all sectors of the Australian economy and areas of society, it is imperative that regulators and government entities coordinate their efforts.

The Discussion Paper notes the regulatory sandbox models adopted in the EU and United Kingdom (UK).[6] auDA considers a one-stop multi-regulator sandbox approach similar to that proposed and piloted by the UK Government,[7] would allow for genuine cross-pollination of concepts and ideas and support better coherence between different policy areas and better regulatory outcomes through better informed regulators and governments.

It would also help relevant Australian regulators and policymakers to adopt a flexible approach to keep pace with the rapidly evolving nature of AI. Lastly, it would enable them to assess how existing (non-)regulatory frameworks apply to AI systems, and identity potential barriers and challenges that may require amendments to such framework and/or the development of new frameworks. This approach might also lower the costs of effective participation in the development of policies and regulatory frameworks.

We note that the Australian Securities and investments Commission (ASIC) is operating an Enhanced Regulatory Sandbox (ERS) also referred to as 'fintech sandbox' to test innovative financial or credit services. ERS 'best practices' and 'lessons learned' could inform a multi-regulator sandbox for AI systems and applications.

A multi-regulator sandbox could also help promote innovation and support increased market participation by small and medium-sized enterprises (SMEs) in the development of AI applications. Supporting SMEs in participating in the digital economy must be a government priority. Therefore, sandbox access should be as open as possible.

A multi-regulator sandbox could benefit from the adoption of a multi-stakeholder approach (see also our **Other areas of relevance** section). By including stakeholders such as the technical

[5] The Tech Policy Design Centre's Tech Policy and Regulation Coordination Model proposed such an approach. For more information, see TPDC_Cultivating_Coordination_2_20230221.pdf (techpolicydesign.au) (accessed on 27 June 2023).
[6] See p. 29 in Discussion Paper.
[7] For more information, see also: https://www.gov.uk/government/publications/projects-selected-for-the-regulators-pioneer-fund/projects-selected-for-the-regulators-pioneer-fund-2022#project-led-by-the-information-commissioners-office (accessed on 10 July 2023).

community, academia, and relevant non-government organisations in the sandbox, regulators and policymakers would benefit from a wider perspective on the potential risks, benefits, and practical considerations associated with AI by different stakeholder segments.

Such inclusiveness would promote a sense of ownership and legitimacy, enhancing public trust and acceptance of AI (see also auDA's response to **Q11**).

Regulatory coordination and collaboration should not be limited to the domestic policy environment. auDA generally supports cross-border cooperation and harmonisation of frameworks to align with international best practices. Harmonisation and interoperability between equivalent global regulatory regimes provide greater legal certainty for Australian businesses and individuals, avoid unnecessary barriers to innovation, and encourage adoption of AI.

Potential bans of high-risk AI Applications (Q10)

Without specifying contextual parameters, auDA believes that for ethical reasons and to protect Australians' fundamental rights, bans should be considered for AI applications that pose unacceptable risks to Australians and their digital wellbeing.[8] Such bans would not only protect individuals' rights and wellbeing but also help maintain and enhance their trust in the technology (see also auDA's response to **Q11**).

auDA understands that Article 5 on Prohibited Artificial Intelligence Practices in the EU's AI Act contains a clear statement on systems deemed to pose unacceptable risks such as real-time biometric identification systems in public spaces, being prohibited with little exception.[9]

When considering bans, it is important to clearly define the precise AI applications or 'use cases' that would fall under such bans to avoid hampering innovation.

Overall, auDA believes that such provisions could also be helpful to enhance cyber hygiene and improve privacy across the digital economy. The less data - particularly sensitive information - is collected and retained, the less vulnerable to cyber threats governments, businesses and individuals are likely to be.

Government initiatives to increase public trust in AI (Q11)

auDA notes that Attachment C of the Discussion Paper outlines several 'elements' useful to increase public trust in AI (e.g., impact assessments, notices, human oversight, explanation, training, monitoring and documentation).

---

[8] These views are aligned with policy opinions expressed by the Australian Human Rights Commission (AHRC) (see e.g., AHRC's submission to the Attorney-General's Department Privacy Act Review Report 2022)

[9] For more information, see https://www.europarl.europa.eu/news/en/press-room/20230609IPR96212/meps-ready-to-negotiate-first-ever-rules-for-safe-and-transparent-ai (accessed on 7 July 2023).

Some of those initiatives would be particularly important from a cyber security perspective, which in turn would increase trust in AI systems. As an example, oversight of AI systems is necessary not only to monitor whether algorithms are operating as intended, but also to detect abnormal algorithmic behaviour due to cyberattacks. Considering privacy concerns, a data quality assessment (including data traceability) adds value to assure Australians' personal information is not misused.

Through targeted initiatives, the Government should encourage trustworthiness features of AI such as oversight, data accuracy and traceability, explainability and transparency that inherently support and complement cyber security.

auDA believes that sustained acceptance and adoption of AI in society are founded on peoples' trust in and understanding of the technology. Australians have a low level of awareness of what AI is and what it means.[10] A concerted effort by Government is needed to raise public awareness of what AI is and what it isn't, what it can be used for and what it mustn't be used for.

It is important for civil society to have a general understanding of the systems they engage with to foresee consequences, engage in debate, and potentially challenge outcomes when users are adversely affected. This is key in developing public acceptance and confidence in the technology.

Suitability of a risk-based approach for AI (Q14)

auDA believes that a risk-based approach is sensible, meaning that the requirements for AI systems would be proportionate to the risk in the respective areas of application. auDA considers such an approach can largely be achieved without creating unnecessary additional regulatory burden that may lead to higher compliance costs compliance or hamper innovation.

Other areas of relevance

Cyber security implications

The Discussion Paper does not intend to address all threats and risks posed by AI.[11] However, auDA believes that attention should be paid to the cyber security implications of AI applications.

From a cyber security perspective, AI is a double-edged sword: it can be deployed for cyber security defence as much as for cyber security disruptions.

[10] See e.g., AIIA and KPMG (2023): Navigating AI – Analysis and guidance on the use and adoption of AI, May 2023, available at: https://aiia.com.au/wp-content/uploads/2023/03/KPMG-and-AIIA-_Navigating-AI-REPORT.pdf (accessed on 6 July 2023).
[11] See p. 4 in Discussion Paper

auDA understands that AI can help improve malware performance by creating and automating threats that are more credible to victims. In turn, this allows for more tailored phishing attacks that can mimic trusted sources with higher precision. Australians will find it more difficult to identity threats and protect themselves. The emergence and fast uptake of generative AI exacerbates such risks.

Addressing cyber security risks is essential for building public trust in AI (see auDA's response to **Q11**). Cyber security risks go beyond national security flagged in the Discussion Paper.[12] They are risks faced by all Australians using AI applications – whether it is for professional or personal purposes.

auDA notes that the development of the 2023-2030 Australian National Cyber Security Strategy and the review of the Privacy Act are ongoing. Both reforms will have implications for the work the Department is undertaking on safe and responsible AI. auDA suggests that the Department coordinates its efforts with the Attorney-General's Department on privacy reform matters, and the Department of Home Affairs of cyber security reform matters.

Multi-stakeholder discussions

auDA acknowledges the establishment of the National AI Centre bringing together government entities, industry and academia to develop Australia's AI ecosystem. auDA suggests that such coordination efforts could be expanded and complemented by a more inclusive multi-stakeholder approach that would see *all* relevant stakeholder groups including regulators and government entities, the technical community, businesses, academia and the public actively participate in AI governance debates (see also auDA's response to **Q4**).

Multi-stakeholder discussions can also encourage international collaboration and the alignment of policy and regulatory approaches across borders. By engaging and collaborating with stakeholders from different countries, regulators can work towards harmonising AI governance principles, regulations and standards, promoting interoperability, and avoiding unnecessary barriers to trade and innovation.

The **2023 Asia Pacific Regional Internet Governance Forum (APrIGF)** to be held in Brisbane from 29-31 August 2023, will feature several sessions on AI and related topics including the challenges of responsible innovation, accessibility, cyber security and governance. Adopting the multi-stakeholder approach as its core principle, the APrIGF event provides a platform for knowledge exchange and collaboration at a regional level to advance internet governance development and digital transformation in the Asia Pacific region. The event will bring participants from the

[12] See also auDA's blog post on Australia's National Cyber Security Strategy summarising auDA's policy position on the 2023-2030 Australian National Cyber Security Strategy: https://www.auda.org.au/blog/australias-national-cyber-security-strategy (accessed on 11 July 2023).

multi-stakeholder internet community across the Asia Pacific region, including government officials, civil society representatives, industry leaders, technical experts and academics.

Given the Government's focus on engagement with our Pacific neighbours and its initiatives and interest in AI and other emerging technologies, auDA would welcome the Government's participation in the APrIGF and its support in bringing the Asia Pacific internet community together. Building stronger connections with Asia Pacific counterparts would help to better position Australia in the global policy debate about AI as well as other emerging technologies.

Conclusion

Overall, it is auDA's view that all relevant stakeholders should be involved in inclusive multi-stakeholder engagements to develop AI governance tools that will ensure the technology is secure and used responsibly. Secure AI systems will promote trust in AI and, in turn, accelerate Australia's digital transformation and enhance Australians' digital wellbeing.

If you would like to discuss our submission, please contact auDA's Internet Governance and Policy Director, Jordan Carter on jordan.carter@auda.org.au.

.au Domain Administration Ltd
www.auda.org.au

PO Box 18315
Melbourne VIC 3001
info@auda.org.au