Australian Government

Office of the Australian Information Commissioner

Department of Industry, Science and Resources – Safe and Responsible AI in Australia Discussion Paper

Submission by the Office of the Australian Information Commissioner

Angelene Falk

Australian Information Commissioner and Privacy Commissioner

18 August 2023

OAIC

Contents

Introduction

1. The Office of the Australian Information Commissioner (the OAIC) welcomes the opportunity to comment on the 'Safe and responsible AI in Australia' Discussion Paper (the Discussion Paper) released by the Department of Industry, Science and Resources (DISR).

2. The OAIC is an independent Commonwealth regulator within the Attorney-General's portfolio, established to bring together three functions: privacy functions (protecting the privacy of individuals under the *Privacy Act 1988* (Cth) (Privacy Act) and other legislation), freedom of information functions (access to information held by the Commonwealth Government in accordance with the *Freedom of Information Act 1982* (Cth)), and information management functions (as set out in the *Australian Information Commissioner Act 2010* (Cth)).

3. Artificial intelligence (AI) has the potential to deliver significant benefits for the economy and society.[1] It is already integrated with the daily lives of Australians, changing the way we work, learn and socialise.[2] Examples include using facial recognition to open your phone or tailoring of a news feed.[3] However, the data-driven nature of AI technologies, which rely on large data sets that often include personal information, can also amplify privacy risks.

4. The Discussion Paper provides that Australians' adoption of AI has remained relatively low, with one reason being low levels of public trust and confidence in AI.[4] The OAIC has also identified significant community concern with the use of personal information in AI systems. The OAIC's 2023 Australian Community Attitudes to Privacy Survey (ACAPS) found that 43% of Australians consider that AI using their personal information to be one of the biggest privacy risks they face today.[5] In addition 54% of Australians are uncomfortable with government agencies using AI to make decisions about them using their personal information and 61% of Australians are uncomfortable with private sector organisations using their personal information in this way.[6]

5. The Discussion Paper notes that building public trust and confidence in the community involves consideration of whether further regulatory and governance responses are required to ensure appropriate safeguards are in place. We note that one of DISR's objectives in the Discussion Paper is to understand the extent to which our existing regulatory frameworks and reform processes already provide (or may be reformed to provide) safeguards against the risks presented by AI. We support this approach and the consideration of how existing frameworks can be strengthened and enhanced to provide adequate safeguards before consideration is given to create a separate regime specific to AI.

6. The Privacy Act provides a well-established framework to minimise the privacy risks associated with personal information handling and facilitate community trust and confidence in new

---

[1] Throughout this submission we use artificial intelligence or AI as a general term to refer to the broad range of related technologies, unless otherwise specified. We note that some related technologies such as automated decision-making, will not always use AI technology. Where necessary, we have referred to these specific technologies by their name.

[2] Office of the Victorian Information Commissioner (OVIC), *Artificial intelligence and privacy*, OVIC website, August 2018.

[3] See Karen Panetta and Guangjie Han, '10 Uses of AI in Everyday Life', *IEEE Transmitter*, 29 December 2022 (updated 21 April 2023), accessed 9 August 2023.

[4] Department of Industry, Science and Resources (DISR), *Safe and Responsible AI in Australia*, DISR, p 3.

[5] Lonergan Research, *Australian Community Attitudes to Privacy Survey 2023*, report to OAIC, August 2023, p 24.

[6] Lonergan Research, *Australian Community Attitudes to Privacy Survey 2023*, report to OAIC, August 2023, p 78.

technologies and data initiatives. The OAIC's 2023 ACAPS results show that 69% of Australians consider compliance with strict privacy rules to be an essential precondition to organisations using artificial intelligence to make a decision that could affect them.[7]

7. This submission focusses on the role that privacy plays in building trust and confidence in the adoption of new and emerging technologies like AI, and our views on measures that can further support this objective by strengthening the existing privacy framework through the Attorney-General's Department's (the Department's) ongoing review of the Privacy Act (the Privacy Act Review). It also considers the need to ensure a multi-faceted regulatory approach, complementing the separate joint submission of the Digital Platform Regulators Forum (DP-REG).

Australia's privacy framework

8. The Privacy Act is principles-based and technology neutral, which enables it to apply to the handing of personal information across a diverse range of technologies. Privacy obligations will apply where personal information is used to train, test or deploy an AI system. The Privacy Act contains Australian Privacy Principles (APPs), which apply to Australian Government agencies and private sector organisations with an annual turnover of more than $3 million subject to some exceptions (APP entities).[8] The APPs outlines how APP entities are permitted to handle personal information and are structured to reflect the information lifecycle, from collection, through to use and disclosure, storage and destruction.

9. The technology neutral application of the APPs allows for 'future-proofing', which preserves the relevance and applicability of the APPs as technology changes.[9] For example, the OAIC's Guide to data analytics and the Australian Privacy Principles provides guidance on the application of the APPs to modern data analytics despite significant advances in the generation and treatment of data since the APPs commenced nearly a decade ago.[10] This is an essential feature of any future-focused regulatory model given the 'speed of innovation in recent AI models'.[11]

10. The principles-based nature of the APPs provides APP entities with the flexibility to take a risk-based approach to the protection of individuals' privacy, having regard to their particular circumstances, including size, resources and business model. This enables the APPs to be scalable and adaptable to the different acts, practices and technologies of APP entities while, importantly, allowing APP entities to simultaneously innovate and carry out their functions and activities. It also allows the Privacy Act to complement other legislation or regulatory frameworks that may deal with related issues.

11. The Privacy Act contains mechanisms that allow the APPs to be supplemented by more specific rules in regulations or other legislative instruments, in appropriate circumstances. For example,

---

[7] Lonergan Research, *Australian Community Attitudes to Privacy Survey 2023*, report to OAIC, August 2023, p 77.

[8] *Privacy Act 1988* (Cth) ss 6(definition of 'APP entity'), 6C and 6D. The Privacy Act Review also proposes removing the $3 million threshold such that organisations will be subject to the Privacy Act regardless of their turnover.

[9] OAIC, *Australian Privacy Principles guidelines*, OAIC website, July 2019, accessed 9 August 2023.

[10] OAIC, *Guide to data analytics and the Australian Privacy Principles*, OAIC website, 21 March 2018, accessed 9 August 2023.

[11] DISR, *Safe and Responsible AI in Australia*, DISR, p 3.

APP codes can adapt and particularise the APPs where appropriate, providing greater clarity about obligations where that is warranted by the entity's particular circumstances.[12]

12. The risk-based approach in the Privacy Act is further enhanced by the obligation, under an enforceable code, for Australian Government agencies to conduct a Privacy Impact Assessment (PIA) for all high privacy risk projects.[13] By way of example, a 'high privacy risk activity' may include the collection, use or disclosure of personal information for automated decision-making with legal or similarly significant effects or for personalised advertising.[14]

13. A PIA is a systematic assessment of a project which can assist in identifying potential privacy impacts that the project might have on individuals, and sets out recommendations for managing, minimising or eliminating those impacts.

14. The OAIC provides guidance to entities conducting a PIA, which provides that privacy risks and impacts should be considered early in a project to influence project design, considering whether the privacy impacts of an activity are necessary and proportionate, and ongoing management of privacy risks.[15] It also encourages consideration of broader privacy implications beyond strict privacy compliance, such as whether a planned use will be acceptable to the community.

15. In this way, PIAs facilitate a privacy by design approach, which considers privacy from the start and then throughout the information lifecycle, rather than being bolted on afterwards.

16. Good privacy practices that meet community expectations through compliance with the Privacy Act and the APPs will help to create the trust and confidence that is needed for the public to engage with AI technologies.

Enhanced privacy protections

17. The Privacy Act Review report contains 116 proposals that seek to ensure that the Privacy Act is fit for purpose in the digital age. The Discussion Paper identifies proposals in the Privacy Act Review report which aim to directly enhance transparency in entities' use of AI.[16] In addition to these technology-specific proposals, we take this opportunity to highlight other proposals in the Privacy Act Review report that would also operate to mitigate the privacy risks associated with AI by raising the standard of personal information across the economy.

Increased accountability for APP entities

18. The Privacy Act Review report includes important proposals that seek to shift the burden from individuals to protect themselves from harm by increasing the accountability of entities for their

[12] *Privacy Act 1988* (Cth) Part IIIB.

[13] *Privacy (Australian Government Agencies – Governance) APP Code 2017* (Cth), cl 12.

[14] AGD, *Privacy Act Review – Report*, AGD, 2022, p 124 proposes an indicative list of high privacy risk activities that could be listed in the Privacy Act or OAIC guidance.

[15] OAIC, *Guide to undertaking privacy impact assessments*, OAIC website, 2 September 2021, accessed 9 August 2023.

[16] Box 1 sets outs proposals 19.1, 19.3, 20.3 and 20.9 of the Attorney-General's Department (AGD), *Privacy Act Review – Report*, AGD, 2022.

personal information handling activities, which is particularly important in the context of complicated information handling practices within AI systems.

19. This includes the proposal to establish a positive obligation on organisations to collect, use, and disclose personal information fairly and reasonably.[17] The OAIC views this proposal as a new keystone for the Privacy Act. It would require entities to proactively consider whether their personal information handling activities are appropriate and set a baseline standard of information handling that is flexible and adaptable as circumstances and technology change.

20. For example, an activity that may be unfair or unreasonable under the proposed obligation may include a financial institution using an AI model to automate a financial service application. If that AI model uses an applicant's personal information to infer other information about them, it may be unfair or unreasonable for that inferred information to be incorporated into the AI's decision-making process, particularly where the individual did not expect their personal information to be used in this way.

21. Similarly, an AI system using individuals' personal information to set different prices in an advertisement for the same product may not be fair and reasonable.

22. In the OAIC's view, a positive obligation for organisations to handle data fairly and reasonably would give individuals engaging with AI technologies greater confidence that they will be treated fairly, and that—like a safety standard—privacy protection is assured. The principles-based nature of the proposed obligation also provides entities with the flexibility to innovate and contribute to a thriving digital economy. The proposal also recognises an exception where collection, use or disclosure is required or authorised by law.

23. Another key proposal to increase organisational accountability that all APP entities would be required to complete a PIA prior to undertaking any 'high privacy risk activity'.[18] Requiring all APP entities – not just Australian Government agencies - to comply with this obligation encourages a privacy by design approach across the economy, fostering public trust and confidence.

24. The above proposals are supported by additional proposals, including requiring entities to document the purposes for which information will be collected, used or disclosed, and appointing a senior employee who is responsible for privacy.[19] These requirements would encourage entities to carefully consider their data handling and foster a culture of respect for privacy and the value of personal information. We consider they will drive behavioural change in how all APP entities, including those that use AI technology, approach privacy.

---

[17] AGD, *Privacy Act Review – Report*, AGD, 2022, proposal 12.1.

[18] The test would align with the circumstances in which a PIA is required under clause 12 of the *Privacy (Australian Government Agencies – Governance) APP Code 2017* (Cth). A 'high privacy risk activity' is 'any function or activity that is likely to have a significant impact on the privacy of individuals' - see AGD, *Privacy Act Review – Report*, AGD, 2022, proposal 13.1 and p 124.

[19] AGD, *Privacy Act Review – Report*, AGD, 2022, proposals 15.1 and 15.2.

Strengthening individuals' control of their personal information

25. Personal information handling in AI is often opaque and complex. Transparency enables individuals to have knowledge, choice and control over how information about them is handled by APP entities. Most Australians see transparency about when AI is being used, and a right to request information about how AI decisions are made, as essential preconditions for the use of AI to make decisions.[20]

26. The Privacy Act Review report includes a number of proposals to promote transparency in personal information handling. In addition to the measures identified the Discussion Paper, this includes measures to improve notices provided to the individual about how their personal information will be used and how their information is collected, used or disclosed for any high privacy risk activities.[21]

27. These transparency measures will also enable individuals to exercise their other rights, such as the proposed new rights to request an explanation of what an entity has done with their personal information,[22] to object to or challenge information handling practices and to request erasure of personal information.[23] These bolster the tools available to individuals to exercise meaningful choice and control over their personal information.

Enabling effective enforcement

28. Effective enforcement is essential to protecting the privacy of individuals and the public interest in privacy.[24] The new regulatory tools proposed in the Privacy Act Review report, together with sufficient resourcing, will enable the OAIC to continue to uphold the law and respond to privacy threats in a timely, proportionate and pragmatic way, including where AI technologies are involved.

29. These proposals include a new mid-tier civil penalty for interferences with privacy without needing to meet the threshold of being 'serious' or 'repeated', infringement notice powers for administrative breaches of the Privacy Act and stronger information gathering powers to increase the OAIC's enforcement capabilities.[25] The OAIC is conducting a strategic review that considers what is needed, both now and in the future, to be a contemporary regulator and to use these powers where appropriate to meet the community expectations for privacy regulation.

30. These enhancements would build on the changes to the OAIC's enforcement powers made by the *Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022* (Cth) including significantly increased penalties for serious and/or repeated privacy breaches, greater information sharing powers and amendment to the extraterritoriality provisions of the Privacy

---

[20] Lonergan Research, *Australian Community Attitudes to Privacy Survey 2023*, report to OAIC, August 2023, p 77.

[21] AGD, *Privacy Act Review – Report*, AGD, 2022, proposals 10.1 and 10.2.

[22] AGD, *Privacy Act Review – Report*, AGD, 2022, proposal 18.1.

[23] AGD, *Privacy Act Review – Report*, AGD, 2022, proposal 18.3.

[24] AGD, *Privacy Act Review – Report*, AGD, 2022, p 252.

[25] AGD, *Privacy Act Review – Report*, AGD, 2022, proposals 25.1, 25.2, and 25.3.

Act to require foreign entities carrying on a business in Australia to comply with the Privacy Act.[26]

31. Together, these changes to the Privacy Act's enforcement framework support enforcement of privacy rights in a timely and effective manner and deter entities from engaging in practices that risk breaching their privacy obligations.

The risk-based approach model

32. One of the possible regulatory responses explored in the Discussion Paper is a risk-based approach to addressing the risks of AI. The risk-based approach is based around 6 themes—impact assessments, notices, human in the loop/oversight assessments, monitoring and documentation, explanations and training.[27] The Discussion Paper considers that this risk-based approach would cater to the context-specific risks of AI, allowing the requirements to change depending on how the AI is deployed and the nature of the AI's impacts on individuals.

33. The Discussion Paper asks submitters for input on how an AI risk-based approach can be incorporated into existing assessment frameworks (like privacy) or risk management processes to streamline and reduce potential duplication. Several of the suggested elements of the proposed risk-based approach have parallels with existing obligations under the Privacy Act and proposals in the Privacy Act Review report. For example, an 'AI impact assessment' is similar to a PIA in that both require entities to appropriately consider and mitigate the potential risks and impacts of a project, and the documentation obligations in the risk-based approach may contain similar information to mapping of information flows in a PIA. Similarly, the notice and explanation elements in the proposed risk-based approach may require provision of similar information to existing or proposed requirements for notice and explanation in the Privacy Act.[28]

34. Given these parallels, we support streamlining the requirements for AI-related activities to avoid placing duplicative obligations on entities and to simplify the regulatory regime for consumers. Depending on the outcome of this consultation, this could take place through guidance on how best to leverage the Privacy Act's notice and explanation requirements to support the same requirements in an AI risk-based approach.

Global interoperability

35. The Discussion Paper notes that our ability to take advantage of AI supplied globally and support the growth of AI in Australia will be impacted by the extent to which Australia's safeguards and responses to AI are consistent with overseas legal and regulatory regimes.

36. Personal information flows across national borders, so having a robust data protection framework, which is interoperable across international regulatory regimes, will be key to mitigating the privacy impacts of AI technologies. This alignment can facilitate engagement of multinational businesses in the Australian economy by creating predictable, globally aligned

---

[26] *Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022*(Cth) s 14.

[27] The model is set out in Box 4 and details of the requirements and obligations are set out in Attachment C of the Discussion Paper.

[28] AGD, *Privacy Act Review – Report*, AGD, 2022, proposals 10.2, 18.1, 19.1, 19.3 and 20.9; *Privacy Act 1988* (Cth) APP 5.

privacy requirements. Interoperable frameworks will also support effective cross-border regulation.

37. Interoperability does not necessarily mean adopting international laws in totality in Australia. Instead, it is important to consider how to create consistently high global privacy standards, and what elements may suit the Australian economy and support that objective.

38. The privacy issues raised by AI systems are not unique to Australia and are also being considered by data protection authorities internationally. The OAIC actively engages with its counterparts in relation to these issues through bilateral and multilateral relationships, including through its membership of the Global Privacy Assembly, Asia Pacific Privacy Authorities, the Common Thread Network and the Global Privacy Enforcement Network. The OAIC is a member of the Global Privacy Assembly's Ethics and Data Protection in Artificial Intelligence working group, which considers developments regarding AI, ethics and data protection globally, including policy initiatives to regulate AI.

39. Our engagement with these fora helps to ensure an interoperable, coordinated, contemporary and best practice approach to regulation. Through these relationships, the OAIC monitors global developments, engages in joint enforcement action and develops best practice principles where appropriate.[29]

Regulatory cooperation

40. We also recognise the importance of domestic collaboration in this area. The OAIC has observed growing intersections between domestic frameworks relating to data and digital technologies, including privacy, competition and consumer law, and online safety and online content regulation. While there are synergies between these frameworks, there are also variances given each regulatory framework is designed to address different economic and societal issues.

41. Where different regulators exercise different functions under various laws it is important for regulators to work together to avoid any unnecessary or inadvertent overlap and uncertainty for consumers and industry. At the same time, we do not consider that regulatory overlap is necessarily a negative outcome, particularly where it is well managed. It is more problematic if regulatory gaps expose individuals to harm or lead to inconsistent and inefficient regulatory approaches.

42. An effective approach must address the importance of institutional coordination between different regulatory bodies in different areas, given the need for complementary expertise.

43. To this end, the OAIC has entered into MOUs with other regulators including the ACCC, Australian Communications and Media Authority (ACMA), Australian Digital Health Agency and the Inspector-General of Intelligence and Security. The OAIC is also a member of DP-REG, together with the ACCC, ACMA and Office of the eSafety Commissioner. As set out further in DP-REG's joint submission to this Discussion Paper, members share information about, and collaborate on, cross-cutting issues and activities on the regulation of digital platforms,

[29] See for example Global Privacy Assembly, *Resolution on Principles and Expectations for the Appropriate Use of Personal Information in Facial Recognition Technology*, Global Privacy Assembly, October 2022.

including in relation to AI used by digital platforms. This promotes a consistent and coordinated approach.

Conclusion

44. The Privacy Act is a principles-based and technology neutral framework through which Australians' privacy rights are protected and privacy obligations are imposed on certain entities, including those that use AI technology. The current Privacy Act Review is an important opportunity to enhance the privacy framework and to ensure Australia's privacy settings empower individuals, protect their personal information and best serve the Australian economy in the digital age. Many of these proposals would help to address the privacy risks presented by AI technology.

45. To the extent that DISR identifies any gaps in privacy regulation to respond to the needs of AI technology, we recommend that DISR considers how best to resolve these through the framework of the Privacy Act. As the regulator of the Privacy Act and an active participant in domestic and global conversations on AI systems, the OAIC is well-equipped to assist DISR to understand the applicability of the current Australian privacy framework and its proposed reforms to the privacy risks of AI technology.