Submission to the Consultation on the APP 1 ADM Obligation

Submission contributors

[redacted]

Contributors

1. The contributors to this submission are legal academics within the Queensland University of Technology's law school with expertise in privacy, artificial intelligence (AI) and automated decision making (ADM). Professor [redacted] primary research interests are privacy, information privacy law and the regulation of information security. [redacted] researches the regulation of ADM and AI and teaches privacy and cybersecurity law. [redacted] research interests are children's rights and privacy law. The views in this submission are our own, and do not represent those of the Queensland University of Technology.

Recommendations

2. Adopt a principled approach to understanding 'meaningful' information for ADM disclosures as outlined in the UK's Information Commissioner Office's (ICO) guidelines[1] and the European Union's Working Party on the Protection of Individuals With Regard to the Processing of Personal Data (Article 29 Working Party Guidelines)[2].

3. Read Australian Privacy Principle (APP) 1.7 -1.9 in context of APP 1 as a whole and the broader accountability requirements of APP 1.1 and 1.2, as well as the interaction with other APPs, particularly in relation to fair collection and rights to access and collect personal information. For reasons noted below, the gap between the ADM obligation and the requirements of the ICO guidelines and the Article 29 Working Party Guidelines is not as significant as perceived in the Issues Paper because APP 1 requires measures relating to accountability and transparency. It would also put Australia in line with international best practice.

4. Guidance should encourage APP entities to provide information in privacy policies about the effects of ADM, rather than merely providing atomised information about types of personal information used in ADM and the kinds of decisions made by partial or full ADM.

5. Adopt a broader interpretation of ADM risks and harms that specifically identifies privacy-related harms, including collective harms and harms to autonomy, thus bringing the ADM obligation more in line with the *Privacy and Other Legislation Amendment Act 2024 (Cth*) (POLA) Explanatory Memorandum (EM).

6. The final version of the guidelines should indicate how the 'fictional edge cases' could give rise to APP considerations.

Introduction

7. We welcome the opportunity to provide a submission on this important topic. At the onset, we acknowledge the challenging position the Office of the Australian Information Commissioner (OAIC) finds itself in by having to provide concrete guidance when the law reform process is incomplete. It

[1] Information Commissioner's Office and The Alan Turing Institute, *Explaining Decisions Made with AI* (Guidance, 20 May 2020).

[2] Article 29 Data Protection Working Party, *Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679* (WP251rev.01, 6 February 2018). The ICO guidelines draw on the Article 29 Working Party guidance noted above at footnote 1 and thus reflects European international best practice.

is unfortunate that the Government's staged approach to implementing agreed-to proposals from the Privacy Act Review means that the OAIC and stakeholders are having to make decisions on how the ADM provision should apply when the reform process is nowhere near complete.

8. The OAIC is therefore tasked to produce guidance about privacy policy provisions which have been introduced without the important, complementary provisions that were proposed alongside them: e.g. fair and reasonable processing, amendments to the definition of personal information and the introduction of rights of access and explanation. Ideally, however, guidance about the new ADM provisions would direct APP entities to include in privacy policies information about the *effects* of ADM in a manner that would allow individuals to make judgements about whether ADM/information handling is fair and reasonable, and to pursue access and complaints under existing APPs. We appreciate the complications that this unfortunate situation must create.

9. That said, for the reasons set out below, we contend that the final guidance on the ADM provisions should not only consider the increased transparency these obligations bring (which have been the focus of the Issues Paper), but also the corresponding accountability requirements under the *Privacy Act 1988* (Cth) (*Privacy Act*).

10. We believe the ADM obligation needs to be interpreted in the context of APP 1 and APP 1.1-1.2 specifically, as well as the current access and correction rights under APPs 12 and 13, and the overarching obligation of fair and lawful collection under APP 3.5. This broader interpretation of the purpose of the new ADM obligations is in line with the legislative intent of the POLA which introduced the obligation. The POLA EM explicitly states one of the purposes of the new ADM obligation is to 'reduce the risk of discrimination by allowing individuals to request entities correct information held or to take further action if there has been an interference with their privacy or unlawful discrimination.'[3]

11. While transparency is an important value in its own right, APP 1 requires an interpretation that goes beyond transparency to consider other intended compliance requirements of the *Privacy Act*, including accountability. That interpretation is more in line with international best practice, as outlined in the ICO guidelines. Doing so, will ensure that the beneficial intention of APP 1.7-1.9 is in line with the expectations of lifecycle management of personal information at the heart of the *Privacy Act* and most information privacy laws.

12. We appreciate that there is a transparency orientation to the construction of APP 1.7-1.9 but other values central to the application of APP 1 more broadly, accountability and in the future, fairness which requires a broader and principled approach to understand what would be *meaningful information* for an individual. We outline our argument further below before contending a broader interpretation of risk and harm is also required.

13. We also appreciate the innovative approach adopted in the Issues Paper involving fictional case studies and ranking of key terms. We have not followed the approach adopted in the Issues Paper questions because our submission relates to a broader issue of principle which could not have been addressed so thoroughly by answering the individual questions. We commend the OAIC for its

[3] *Privacy and Other Legislation Amendment Bill 2024* (Cth) Explanatory Memorandum, [111].

innovative approach to consultations as exemplified in the ADM obligation and recently in the Children's Online Privacy Code consultation also.

A Principled Approach to 'Meaningful' Explanation

14. The Issues Paper highlights that the ADM obligation gives individuals 'no right to contestability or to request information, and no obligation to notify.'[4] In that regard, the Issues Paper concludes that the obligation is not as extensive as the application of other similar rights of explanation, such as Article 22 of the General Data Protection Regulation (GDPR)[5], its UK equivalent (UK GDPR)[6] and Principle 10 of the *Privacy and Responsible Information Sharing Act 2024* (WA). The Issues Paper also makes clear that the value of transparency broadly underpins the obligation and will assist consumers to 'know when and how best to exercise information access or review options in other frameworks.'[7] To do so effectively, the Issues Paper rightly highlights that APP 1.7-1.9 will require 'a balance between providing enough *meaningful* information for individuals to understand…and avoiding excessive detail that obscures the purpose of transparency and clear communication [emphasis added].'[8] The Issues Paper then considers five disclosure considerations - clear articulation, facilitating further requests, appropriately tailored, logically organised and framed to give rise to contestability.[9]

15. We tentatively agree with the five considerations outlined to generally govern the application of disclosure requirements for APP entities. We think these higher-level considerations are clear and concise enough to guide APP entities on how to provide the kinds of personal information and decisions contemplated by APP 1.8. As noted, however, we believe the guidelines could also emulate the principled approach adopted by the ICO with its deeper focus on meaningful information in an automated and AI context.

16. The question therefore shifts to what information APP entities should provide under APP 1.7-1.8 that would be 'meaningful.' We believe the Issues Paper considers this question granularly, especially in relation to the questions posed. We commend the OAIC for trying to assist submitters to consider the required detail of what could be a meaningful disclosure for individuals that supports the value of transparency.

17. However, rather than focusing on the detail of technically oriented considerations of key term disclosures, specifically, 'substantially and directly related' and 'arranged for a computer program', we believe that the application of a principled approach to considering what information would be meaningful considering the purpose of APP 1 as a whole would be more beneficial, as it will ensure that the application of the obligation is in line with international best practice. Doing so, will also give

---

[4] Office of the Australian Information Commissioner, *Automated Decision-making Transparency Obligation (APP 1): Issues Paper* (2023), 10.

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [2016] OJ L 119/1.

[6] Regulation (EU) 2016/679 as it forms part of domestic law under the European Union (Withdrawal) Act 2018 (UK) (UK GDPR).

[7] Office of the Australian Information Commissioner, *Issues Paper* (n 4) 8.

[8] Ibid 21.

[9] Ibid 23-24.

rise to a broader understanding of the ADM obligation that entails an accountability requirement due to its placement in APP 1, and its interaction with other APP obligations.

18. If APP entities already have good practices in place they should be able to identify easily what kinds of ADM need to be included. However, where entities do not have a good understanding of the ADM occurring, they will need to implement practices, procedures and systems to ensure they can comply with the new obligation. The focus on meaningful information should therefore aim to send a clear compliance signal based on the principles of transparency **and** accountability rather than refer to a distinct phrasing or combination of words.

19. The Issues Paper helpfully acknowledges and references the UK ICO guidance, in conjunction with The Alan Turing Institute, on 'Explaining decisions made with AI.'[10] The guidance is designed to assist covered entities under Article 22 of UK GDPR,[11] which like its EU counterpart, is a seemingly broader protection that the proposed ADM obligation. The breadth is visible because the value of transparency at the heart of Article 22 is also intertwined with the values of fairness and accountability, which means that the ICO guidance takes a broader and principled perspective on what is meaningful explanation[12] and why it is important, especially for the flourishing of fully informed members of the public.[13]

20. The breadth of the principled approach allows the ICO to outline a clear distinction between process and outcome explanations and then identify six different types of explanation across a range of different approaches. These include explanations by - rationale; role responsibility; data used; fairness; safety and performance and impact.[14] The Issues Paper also highlights six AI decision-making elements flowing from the different types of explanation and outlining the contextual application at the heart of the ICO's guidance, including understanding meaningfulness that is proportionate to impact and properly tailored to meet specific audiences, such as children.[15]

21. We agree with the Issues Paper about the helpfulness of the ICO's guidance and we contend it provides a good framework for the OAIC and APP entities to use regarding the future application of the ADM obligation.'[16]

22. The breadth of the ICO's guidance is also appropriate for another reason. APP 1.4 already requires APP entities to include in privacy policy information about the kinds of personal information that the entity collects and holds; how the entity collects and holds personal information; and the purposes for which the entity collects, holds, uses and discloses personal information. If APP 1.8 were read narrowly it would in effect add nothing, or almost nothing to what is already required by APP 1.4. If the significance of the potential effects of ADM decisions is what makes them noteworthy, then

[10] Information Commissioner's Office (n 1).

[11] Information Commissioner's Office, 'Rights Related to Automated Decision-Making Including Profiling' (2022) <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/rights-related-to-automated-decision-making-including-profiling/>.

[12] Information Commissioner's Office (n 1) 23-24.

[13] Ibid 29.

[14] Ibid 33.

[15] Office of the Australian Information Commissioner, *Issues Paper* (n 4) 23.

[16] Ibid.

privacy policies only serve the overarching APP 1 goals of openness and transparency by providing a holistic picture of these effects. By contrast, atomised lists of 'kinds of decisions' and 'kinds of personal information' provide little meaningful understanding to individuals.

23. We therefore believe the OAIC should adopt (or adapt) the ICO's guidance, based on an interpretation of APP 1 as a whole to properly situate how APP 1.7-1.9 should apply. On this interpretation, the transparency requirement of APP 1.7-1.9 should be read in context of the governance requirements of APP 1.1 and 1.2.

24. The POLA EM notes a 'privacy policy is a key tool for meeting the objective of APP 1, which is to ensure that entities manage personal information in an open and transparent way.'[17] We generally agree with this statement and note two further considerations.

25. First, the use of 'key' is important because we believe it indicates that a privacy policy, whilst being significant, is not the only mechanism relevant to APP 1 compliance. APP 1.1 and its focus on managing personal information in an open and transparent way indicates that appropriate management structures are necessary for APP compliance which is reemphasised by APP 1.2.

26. Second, APP 1.2 requires an APP entity to take reasonable steps to 'implement practices, procedures and systems relating to the entity's functions or activities' to ensure compliance across the lifecycle of all APPs and enable the APP entity to deal with inquiries, complaints, as well as requests for access and correction of personal information from individuals. We contend that 'practices, procedures and systems' under APP 1.2 are equally 'key' to the overall governance and operation of APP 1 as privacy policies are to APP 1.1.

27. Both the POLA EM and the Issues Paper only consider the application of APP 1.7-1.9 in the context of APP 1.1, on the basis that it represents the 'objective' of APP 1.[18] This justifies the focus on 'open and transparent' as the basis for the ADM obligation's sole transparency orientation. We believe this is a narrow reading of APP 1.1 for several reasons.

28. First, the full requirement of APP 1.1 and its focus on managing personal information in an 'open and transparent way' indicates that APP 1.1 should be considered as much an accountability requirement as a transparency obligation. In other words, the transparency obligation (e.g. 'transparent') must be situated as part of an accountable management process (e.g., the 'manage' and 'way' components) that is contestable (e.g., the 'open' component). If APP 1.1 was solely a transparency obligation, then it would read 'APP entities must provide information transparently to individuals about how their personal information is handled.' Obviously, this is not what APP 1.1 states because its regulatory focus is not on the provision of information. Instead, APP 1.1 focuses on the requirement for APP entities to 'manage' personal information in a specific way that can be contested, thus APP 1.1 uses a privacy policy as a 'key' transparency tool to enable accountability for non-compliance.

29. Our point is supported by the APP Guidelines which confirms that the 'declared object' of APP 1.1 'enhances the *accountability* of APP entities for their personal information handling practices

[17] Explanatory Memorandum, Privacy and Other Legislation Amendment Bill 2024 (Cth) (n 3) [333].

[18] Ibid.

[emphasis added].'[19] The accountability element of APP 1 as a whole is further outlined because 'APP 1 lays down the first step in the information lifecycle – *planning* and *explaining* how personal information will be handled before it is collected [emphasis added].'[20] Again, the planning and explaining elements clearly speak to the purpose of APP 1 as being a management requirement (e.g., planning) and a transparency obligation (e.g., explaining). As such, we believe that APP 1.1 should be read as providing a broader scope for understanding the purpose and application of APP 1.7-1.9 by reading it in context to the purpose of APP 1 as a whole.

30. Second, we also contend that the governance requirement of APP 1 needs to jointly consider the purpose and application of APP 1.1 **and** APP 1.2. The APP Guidelines state that APP 1.2 imposes 'a distinct and separate obligation upon an APP entity, in additional to being a general state of its obligation to comply with other APPs.'[21] We contend that APP 1.2's 'obligation to comply with other APPs' does not exclude APP 1.

31. The 'proactive steps' required from APP 1.2 is an intrinsic part of APP 1.1's 'managing' personal information and how personal information will be handled 'before it is collected.'[22] In terms of understanding how APP 1's object is to be interpreted and applied, we contend that APP 1.1 and 1.2 should be read together as requiring 'practices, procedures and systems' to facilitate 'open and transparent' management of personal information in an accountable 'way'. Our reading of APP 1's governance object re-emphasises that transparency obligations arising under APP 1 should not be parsed from accountability requirements that are 'constant' in terms of the lifecycle management of personal information arising from all APPs.[23]

32. In our previous submission on POLA to the Legal and Constitutional Affairs Legislation Committee,[24] we highlighted that the Government, while agreeing to implement all three recommendations related to Proposal 19, had only adopted 19.1-19.2 which reduced the accountability capabilities of Proposal 19.[25] The Committee report noted the significant debate regarding this issue and made a further recommendation to include text in the EM to 'make clear that the level of information required in privacy policies is not expected to compromise commercial-in-confidence information' about ADM systems.[26] The Government response recognised 'the importance of increasing transparency for Australians without unduly limiting businesses' ability to carry on their operations'

---

[19] Office of the Australian Information Commissioner, 'Australian Privacy Principles Guidelines' (APP Guidelines, May 2026), [1.1].

[20] Ibid [1.3].

[21] Ibid [1.5].

[22] Ibid [1.3].

[23] Ibid [1.5].

[24] Lisa Archbold and others, Submission to the Legal and Constitutional Affairs Legislation Committee inquiry into the Privacy and Other Legislation Amendment Bill 2024. Parliament of Australia < https://eprints.qut.edu.au/253056/>.

[25] Ibid 7-9.

[26] Senate Legal and Constitutional Affairs Legislation Committee, Parliament of Australia, *'Privacy and Other Legislation Amendment Bill 2024 [Provisions]'* (Report, 2024) <https://parlinfo.aph.gov.au/parlInfo/download/committees/reportsen/RB000502/toc_pdf/PrivacyandOtherLegislationAmendmentBill2024[Provisions].pdf.>.

and agreed to the amendment.[27] None of these considerations indicate why APP 1.7-1.9 should be considered solely as a 'transparency obligation.'

33. Our detailed consideration of APP 1 is used to justify that the distance between the ADM obligation and the ICO principled approach is not as great as made out in the Issues Paper. The situation will be more so when Tranche 2 of *The Privacy Act* reforms is implemented which will bring the new 'fair and reasonableness' requirement to the lifecycle management process of the APPs. Preparing for that situation, re-emphasises that the value of transparency in the ADM obligation should be considered alongside the current accountability requirements of APP 1, fairness requirements in APP 3.5 and rights to request and correct personal information under APP 12 and 13. Framing the initial guidance in this way will ensure APP entities are prepared for, if and when the new 'fair and reasonable' requirements are implemented.

34. All this again points to the fact that the principled approach of the ICO guidelines should be considered as a framework for the purpose and application of APP 1.7-1.9. Doing so, would bring the application of APP 1 in line with international best practice, which was a stated goal of the *Privacy Act* reforms.[28]

35. The ICO guidelines would need to be tailored to the Australian context, but we nonetheless think they are a helpful framework to consider the issue of ADM disclosures more broadly. More importantly, they demonstrate that ADM disclosures would benefit by being considered from a principled position of encouraging broader compliance values across APP entities rather than trying to secure a specific terminological outcome.

36. Finally, if APP 1.7-1.9 is read as being a pure transparency mechanism, based on a reading of APP 1.1 as the 'declared object' of APP 1 more generally, then that could have the future effect of reading in an interpretation of APP 1 that favours the value of transparency at the expense of accountability. As noted above, we do not believe that situation is warranted or desirable moving forward.

A Broader Interpretation of ADM Risks and Harms

37. The Issues Paper rightly notes that individuals can be detrimentally impacted by AI and ADM and that 'a community that is better informed can participate more effectively in democratic processes.'[29] APP 1.7 provides that ADM decisions which could 'reasonably be expected to significantly affect the rights or interests of an individual' must be outlined in a privacy policy in line with the requirements of APP 1.8. APP 1.9(d) then sets out examples of the types of decisions which would require disclosure. The examples provided in POLA and outlined in the EM, do not necessarily match the depth of concerns portrayed in the opening part of the Issues Paper. The Issues Paper's 'fictional edge cases' also understandably build on these examples as the types of situations relevant to the potential application of APP 1.7-1.9.

---

[27] Australian Government, *Australian government response to the Senate Legal and Constitutional Affairs Legislation Committee report: Privacy and Other Legislation Amendment Bill 2024 [Provisions]* (2024).

[28] Attorney-General's Department (Cth), *Privacy Act Review Report* (Report, February 2023), 1 <https://www.ag.gov.au/sites/default/files/2023-02/privacy-act-review-report_0.pdf>.

[29] Office of the Australian Information Commissioner, *Issues Paper* (n 4) 3.

38. These examples are no doubt important, but they do not capture the full gamut of risks and harms that could arise from AI or ADM. Again, the OAIC could benefit from the principled approach adopted by the ICO which outlines the importance of understanding context especially in relation to potential impacts.

39. Understanding the 'domain contexts' of ADM decision use and the potential impacts that could arise from use of personal information in ADM processes allows UK GDPR covered entities to prioritise explanations and how they are delivered.[30] Meaningful disclosure then is contextualised to the type of risk of harm that could arise and can be tailored in different ways to match the potential severity of the risk. This is possible because the ICO framework is constructed at the level of principle which means it is more adaptable to distinct types of risks and harms.

40. A key risk of harm highlighted in the POLA EM is to privacy itself. ADM systems pose privacy risks because they use personal information 'in ways which may have significant impact, with little transparency.'[31] Individual rights relating to access and disclosure of personal information allows protection from 'unlawful or arbitrary interferences with privacy.'[32] Greater transparency of handing practices, including ADM, therefore allows individuals to 'take further action if there has been a breach of their personal privacy.'[33] As such, Part 15 enhances 'the right to privacy.'[34]

41. Given the significant focus in the EM on the use of APP 1.7-1.9 to protect privacy rights in the information privacy context, it is somewhat surprising that the Issues Paper's remedial goal seemingly involves using other legal frameworks for 'information access or review options.'[35] As such, the Issues Paper does not really consider in depth the type of situation involving ADM decisions that 'significantly affect rights or interests' arising from the *Privacy Act* itself. Given that APP compliance is considered at first instance by the Commissioner, it would be helpful if the final version of the guidelines could indicate how the 'fictional edge cases' could give rise to APP considerations.

42. We also note that privacy harms may be diffuse and collective, and this is relevant to evaluating the 'significance' of the effects of ADM more broadly. Very small harms to an individual might result from one APP entity conducting some form of algorithmic profiling. However, if the same patterns of profiling are repeated consistently, these small harms may be aggregated into something more serious. [36] Similarly, harms which are small for each individual may, at scale result in systematic disadvantage to a group. Leading privacy US law scholars, Professors' Danielle Citron and Daniel Solove, contend

> '…sometimes an organization will cause a very small amount of harm but on a very large scale—to hundreds of thousands or even millions of people. From the standpoint of each

[30] Information Commissioner's Office (n 1) 74.

[31] Explanatory Memorandum, Privacy and Other Legislation Amendment Bill 2024 (Cth) (n 3) [48].

[32] Ibid [49].

[33] Ibid.

[34] Ibid [48].

[35] Office of the Australian Information Commissioner, *Issues Paper* (n 4) 8.

[36] See e.g., Karen Yeung, ''Hypernudge': Big Data as a Mode of Regulation by Design' (2016) 20(1) *Information, Communication & Society* 118-136.

individual, the harm is minor, but from the standpoint of society, where the harm to everyone is aggregated, the total amount of harm is quite substantial.'[37]

43. Effects on rights and interests which might not appear significant at an individual level may still collectively disadvantage groups or have large social effects (and individuals have significant interests in these social effects). For instance, ranking algorithms which have small effects on individuals' information feeds, may at scale systematically exclude large groups from important information and perspectives. This is a significant effect on members of that group's individual and collective interests in access to information and participation in public discourse.

44. Scholars also recognise that harms to autonomy and, and not only harms of intrusion or economic harms, like price discrimination, are 'significant' privacy harms.[38] Theories of privacy recognise both that privacy may protect individuals from manipulation and domination, and that 'decisional privacy' e.g., non-intrusion on decision-making, is a key privacy interest.[39] This suggests that, at least in some circumstances, various forms of targeting, profiling and algorithmic manipulation should be considered 'significant' effects for the purposes of APP 1.7(b).

45. Commentary, including from the Article 29 Working Party, recognises the difficulty of drawing bright lines between acceptable and unacceptable, or significant and insignificant forms of manipulation and influence through profiling and targeting. The EU guidance suggest that the following factors may cause automated profiling and manipulation to rise to a sufficient level of significance:

    - The intrusiveness of the profiling process, including the tracking of individuals across different websites, devices and services;
    - The expectations and wishes of the individuals concerned;
    - The way the advert is delivered; or
    - Using knowledge of the vulnerabilities of the data subjects targeted.[40]

46. Profiling and targeting that is communicated via a companion chatbot with whom a user feels a strong sense of connection or even emotional dependency may therefore be more 'significant' than profiling or targeting in search engine results. It will by necessity depend on context.

47. In conclusion, the contextual nature of what could be a 'significant' effect therefore requires a broad understanding of the privacy risks and harms that could emerge through ADM, as reflected in the POLA EM, which also requires a principled approach to 'meaningful' information to better ameliorate potential harm by encouraging APP entities to be transparent and accountable in the articulation of practices related to APP 1.7-1.9.

---

[37] Daniel J. Solove and Danielle Citron, 'Privacy Harms' (2022) 102 *Boston University Law Review* 793, 816.

[38] See e.g. Bert-Jaap Koops et al, 'A Typology of Privacy' (2017) 38(2) *University of Pennsylvania Journal of International Law* 483; Julie E., Cohen, 'Turning Privacy Inside Out' (2019) 20(1) *Theoretical Inquiries in Law* 1.

[39] Neil Richards, *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age* (Oxford University Press, 2015).

[40] Article 29 Data Protection Working Party (n 2) 22.

Disclosure of Generative AI Uses

The first author used MS Copilot 365 to format footnotes. No other generative AI use was employed by the authors in the production of the submission.