Australian Government

Office of the Australian Information Commissioner

Online Safety Act Review Issues Paper

Submission by the Office of the Australian Information Commissioner

Carly Kind

Privacy Commissioner

1 July 2024

OAIC

Introduction

1. The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to provide a submission to the Statutory Review of the *Online Safety Act 2021* (Cth) (Online Safety Act Review).

2. The OAIC is an independent Commonwealth regulator, 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 (FOI) functions (access to information held by the Commonwealth Government in accordance with the *Freedom of Information Act 1982* (Cth) (FOI Act)), and information management functions (as set out in the *Australian Information Commissioner Act 2010* (Cth)).

3. The Online Safety Act Review Issues Paper (the Issues Paper) invites feedback on the operation and effectiveness of the *Online Safety Act 2021* (Cth) (Online Safety Act). It considers its existing regulatory schemes, enforcement mechanisms, regulatory gaps, and international developments in online safety regulation.[1]

4. The Privacy Act and Online Safety Act play distinct and essential roles in addressing the risks and harms faced by Australians in the online environment. While the Privacy Act regulates the handling of personal information by private sector organisations and Australian Government agencies, the Online Safety Act focusses on protecting Australians from online harms resulting from exposure to illegal or harmful online content or behaviour.

5. There are several points of intersection between the two regulatory frameworks. The Privacy Act and Online Safety Act often have complementary objectives, requirements, and approaches. For example, they emphasise the importance of providing individuals with the ability to control their personal information and online safety respectively, as well as embedding privacy and safety protections into the design of services and business practices under a 'privacy by design' and 'safety by design' approach.[2] At times, there may also be competing objectives, whereby a reasonable and proportionate balance should be reached between online safety and privacy considerations.

6. This submission supports the objectives of the Online Safety Act Review and recognises the importance of addressing emerging online safety harms. It also offers observations on the intersections between online safety and privacy considerations, and how a flexible and principles-based approach to online safety regulation allows service providers to achieve both privacy and online safety outcomes. Such an approach ensures that privacy and online safety are not mutually exclusive considerations but are instead complementary components in addressing the risks and harms faced by Australians in the online environment.

[1] Department of Infrastructure, Transport, Regional Development, Communications and the Arts (DITRDCA), *Online Safety Act Review Issues Paper*, 29 April 2024, p 10.

[2] See for example, OAIC, *Privacy by Design*; eSafety Commissioner, *Safety by Design*, 22 April 2024.

Balancing online safety, privacy and human rights considerations

7. The Issues Paper contains the following consultation questions which raise the important intersections between online safety, privacy and broader human rights considerations:

    - *26. Are additional safeguards needed to ensure the Act upholds fundamental human rights and supporting principles?*
    - *28. What considerations are important in balancing innovation, privacy, security, and safety?*[3]

8. The Issues Paper also observes that in regulating the online environment, 'governments must consider how to uphold a range of fundamental human rights and supporting principles' including (among other things), the principle of the best interests of the child, the right to freedom of information, opinion, and expression, the right to privacy and the right to protection from exploitation, violence, and abuse.[4]

9. As stated in the Issues Paper, there are important nuances to be considered in assessing human rights impacts.'[5] The right to privacy is not absolute[6] and in certain circumstances there may be a compelling public interest reason that justifies an impact on privacy in order to achieve other policy objectives. Whether this is appropriate will depend on whether the impact on privacy is reasonable, necessary, and proportionate to pursuing a legitimate objective with a compelling and substantial public interest.[7] Noting that the OAIC's remit also extends to promoting and upholding information access rights (part of the right to freedom of information, opinion, and expression under Article 19 of the *Universal Declaration of Human Rights*) we also emphasise the need to ensure that online safety measures take account of rights to freely impart and receive information. Furthermore, we note that impacts to one human right may have downstream effects on another – for example, significant limitations on the right to privacy can have a chilling effect on freedom of expression.

10. These considerations will be important in relation to any policy proposals or legislative measures arising out of the Online Safety Act Review that may have human rights impacts, particularly privacy impacts. Furthermore, the balance of online safety and privacy considerations (and whether an impact on privacy is reasonable, necessary, and proportionate) may differ between proposals. The OAIC would be pleased to meet with the reviewer to provide its access to information and privacy expertise in balancing these considerations.

Practical examples – Anonymity and age assurance

11. By way of example, the Issues Paper observes that anonymity and identity shielding can protect the privacy and safety of online users but can also 'be used to control and abuse people, and

---

[3] DITRDCA, *Online Safety Act Review Issues Paper*, 29 April 2024, p 44, 54.

[4] Ibid p 43.

[5] Ibid.

[6] See relatedly, *Privacy Act 1988* (Cth) s 2A. See also, OAIC, *What is privacy?*.

[7] See relatedly, Attorney General's Department, *Permissible limitations: Public sector guidance sheet*; Australian Human Rights Commission, *Permissible limitations on rights*.

make it difficult to hold individuals to account.'[8] However, anonymity and pseudonymity are also important privacy principles.[9] An individual may prefer to transact online anonymously or pseudonymously for various reasons including to avoid subsequent contact (such as direct marketing) from an entity, to keep their whereabouts secret from others including in circumstances where they fear harm or harassment from others (such as in domestic violence situations), to access services (such as counselling or health services) without this becoming known to others, or to express views in the public arena without fear of reprisal.[10] In the UK, the Joint Committee on the Draft Online Safety Bill acknowledged concerns in relation to anonymous online abuse but considered that '…anonymity and pseudonymity are crucial to online safety for marginalised groups, for whistleblowers, and for victims of domestic abuse and other forms of offline violence' and that 'ending them would not be a proportionate response.'[11]

12. By way of further example, we note that the Issues Paper asks about the role that the Online Safety Act should play in restricting children's access to age-inappropriate content, including through the application of age assurance.[12] To the extent that the Online Safety Act continues to play a role, we note that a proportionate response requires different approaches to age assurance to be applied, depending on the context and risks in question.

13. From a privacy perspective, the impacts of age assurance or age verification measures are likely to be felt by all Australian users of a service (i.e. adults), not just by the cohort of users who are intended to benefit from increased protections. These impacts must be weighed against the benefits of restricting child access to age-inappropriate content. In this regard, the Office of the Privacy Commissioner of Canada has argued that the use of age assurance systems:

    - Should be restricted to situations that pose a high risk to the best interests of young people; and
    - Must consider impacts on the privacy rights of both young persons and adult users of the online service.[13]

14. We also note there is an important distinction between 'age verification', which refers to measures to determine users' age to a high degree of accuracy, and the broader concept of 'age assurance', which encapsulates age estimation.[14] The former generally entails higher privacy impacts, to the extent that it may require users to submit personal information to verify age (e.g. through identity documents).[15]

---

[8] DITRDCA, *Online Safety Act Review Issues Paper*, 29 April 2024, p 43.

[9] Under Australian Privacy Principle (APP) 2, individuals must have the option of not identifying themselves or of using a pseudonym when dealing with an APP entity, unless it is impracticable for the APP entity to deal with individuals who have not identified themselves or they are required by law to deal with identified individuals. See *Privacy Act 1988* (Cth), APP 2.

[10] See relatedly, OAIC, *Submission to Senate Legal and Constitutional Affairs Legislation Committee – Social Media (Anti-Trolling) Bill 2022*, 10 March 2023.

[11] Joint Committee on the Draft Online Safety Bill, *Draft Online Safety Bill – Report of Session 2021-22*, 14 December 2021, accessed 19 June 2024, p 34.

[12] DITRDCA, *Online Safety Act Review Issues Paper*, 29 April 2024, p 32.

[13] Office of the Privacy Commissioner of Canada, *Privacy and age assurance – Exploratory consultation*, 10 June 2024.

[14] See, Information Commissioner's Office (UK), Age assurance methods, *Age assurance for the Children's code*, 15 January 2024; eSafety Commissioner, *Roadmap for Age Verification*, March 2023, p 16.

[15] Ibid.

15. The OAIC considers that the risk-based approach established by the United Kingdom's *Age Appropriate Design Code* (AADC) represents a proportionate approach.[16] The AADC requires online services to 'establish age with a level of certainty that is appropriate to the risks' that arise from data processing, or to 'apply the standards in this code to all users instead.'[17] The UK Information Commissioner's Office has advised that entities must only use personal information that is necessary to undertake age assurance and must 'consider whether less privacy-intrusive approaches can achieve the same objective'.[18] The AADC therefore allows for measures with less privacy impacts to be applied in lower risk contexts.[19]

16. As is evident through these examples, the balancing exercise required to determine whether a privacy impact is proportionate will necessarily be informed by the particular issue and circumstances at hand, so a 'one-size fits all' approach may not be appropriate.

17. A key method for assessing whether privacy impacts are reasonable, necessary, and proportionate is to conduct a privacy impact assessment (PIA). A PIA is a systematic assessment of a project that identifies the impact it might have on the privacy of individuals (including consideration of community expectations) and sets out recommendations for managing, minimising, or eliminating that impact.[20] The OAIC has developed a suite of guidance materials to assist entities in undertaking PIAs and ultimately design products and services that protect and respect the privacy of individuals.[21]

Recommendation 1 – In balancing privacy, security and safety, the Online Safety Act Review should consider whether any impact on privacy is reasonable, necessary, and proportionate to pursuing a legitimate objective.

A flexible and principles-based regulatory framework

18. The OAIC is supportive of the current flexible and principles-based approach to online safety regulation. In addition to other benefits (e.g. responsiveness to emerging technologies), principles-based requirements allow for the consideration of privacy impacts on a case-by-case basis and enable service providers to adopt proportionate measures.

19. For example, the Basic Online Safety Expectations (BOSE) prompts online service providers to take 'reasonable steps' regarding the safe use of their services, as well as in relation to certain activities and content.[22] This principles-based approach enables online service providers to adopt a flexible and proportionate response to their obligations that achieves both privacy and online safety outcomes. We note that the BOSE do not require or expect service providers to

[16] Information Commissioner's Office (UK), Age appropriate application, *Age Appropriate Design Code*, 17 October 2022. See also, Information Commissioner's Office (UK), *Age assurance for the Children's code*, 15 January 2024.

[17] Information Commissioner's Office (UK), Age appropriate application, *Age Appropriate Design Code*, 17 October 2022.

[18] Information Commissioner's Office (UK), *Age assurance for the Children's code*, 15 January 2024, p 8 and 25.

[19] Ibid p 25.

[20] See, OAIC, *Guide to undertaking privacy impact assessments*, 2 September 2021.

[21] OAIC, *Guide to undertaking privacy impact assessments*, 2 September 2021; OAIC, *Privacy impact assessment tool*, May 2020; OAIC, *Undertaking a privacy impact assessment (e-Learning course)*, 15 May 2017.

[22] Basic Online Safety Expectations Determination 2022 (Cth) ss 6-12.

undertake actions inconsistent with their obligations under the Privacy Act and other relevant laws.[23]

20. This approach broadly aligns with the principles-based framing of the Australian Privacy Principles (APPs). The APPs are not prescriptive and generally require entities to take 'reasonable steps' to meet obligations around the handling of personal information. This approach provides entities with the flexibility to take a risk-based approach to compliance, based on their circumstances, including size, resources, and business model, while ensuring the protection of individuals' privacy.

21. In this way, the Online Safety Act would continue to facilitate an approach in which privacy and online safety are not mutually exclusive considerations but complementary components to address the risks and harms faced by Australians in the online environment.

22. It should be incumbent on industry to develop technological solutions that integrate privacy, security and online safety considerations. Regulatory guidance issued by the eSafety Commissioner will continue to play an important role in supporting industry to achieve these outcomes.[24]

Recommendation 2 – In order to accommodate a balance between privacy, security and safety, the OAIC supports a flexible and principles-based approach to online safety regulation (e.g. requirements to take 'reasonable steps' to achieve an outcome), which enables service providers to adopt proportionate measures that achieve both privacy and online safety outcomes.

Reform of the Privacy Act

23. The Online Safety Act Review comes at a time when the Government has also committed to advancing substantial reform to the Privacy Act.[25] The Attorney-General's Department is progressing several reforms to the Privacy Act which would help to address harms in the online environment, including:

    - A requirement for the collection, use and disclosure of personal information to be 'fair and reasonable in the circumstances'[26]
    - A requirement for entities that provide online services to ensure that privacy settings are clear and easily accessible for service users[27]

[23] See, Explanatory Statement, Online Safety (Basic Online Safety Expectations) Determination 2022, p 4, 9; eSafety Commissioner, Basic Online Safety Expectations: Regulatory Guidance, September 2023, p 8.

[24] See for example, eSafety Commissioner, Basic Online Safety Expectations: Regulatory Guidance, September 2023.

[25] Attorney-General's Department, Government Response to the Privacy Act Review Report, 28 September 2023.

[26] Ibid, Proposals 12.1-12.3.

[27] Ibid, Proposal 11.4.

- A requirement to have regard to the best interests of the child when handling the personal information of children[28]
- The introduction of a Children's Online Privacy Code that applies to online services that are 'likely to be accessed by children' which, among other matters, could address how the best interests of child users should be supported in the design of an online service[29]
- Amendments to the code making powers in the Privacy Act to allow for the Information Commissioner to make an APP Code in additional circumstances, and[30]
- Enhanced enforcement mechanisms and additional avenues for individual redress.[31]

24. The OAIC considers that the Privacy Act reforms and any outcomes from the Online Safety Act Review should progress as soon as possible to ensure comprehensive protection for Australians against privacy and safety harms in the online environment.

25. To the extent that proposals of the Online Safety Act intersect with the proposals of the Privacy Act Review, it will be important for the Department to co-ordinate with the Attorney General's Department to ensure coherence between regulatory frameworks and clarity for the regulated community, as well as for the OAIC and eSafety Commissioner as regulators.

Regulatory cooperation

26. These intersections also highlight the importance of continued co-operation at the regulator level to manage areas of regulatory convergence and ensure clarity for the regulated community. The OAIC has an effective, collaborative and strong working relationship with the eSafety Commissioner, including through our participation in the Digital Platform Regulators Forum (DP-REG).

27. DP-REG is an initiative between the OAIC, Australian Competition and Consumer Commission, Australian Communications and Media Authority and eSafety Commissioner to share information about, and collaborate on, cross-cutting issues and activities on the regulation of digital platforms. This includes consideration of how competition, consumer protection, privacy, online safety, and data issues intersect in order to promote proportionate, cohesive, well-designed and efficiently implemented digital platform regulation.

28. The OAIC will continue to seek opportunities to collaborate with the eSafety Commissioner bilaterally and through DP-REG to promote regulatory outcomes that are consistent with the objectives of the Online Safety Act and Privacy Act.

[28] Ibid, Proposal 16.4.

[29] Ibid, Proposal 16.5.

[30] Ibid, Proposal 5.1-5.2.

[31] Ibid, Chapters 25, 26 and 27.

Conclusion

29. The OAIC is available to engage further with the Online Safety Act Review as it progresses and develops potential reform options. If we can be of further assistance, please contact [redacted]