IPIE
International Panel on the Information Environment

Submission to the Office of the Australian Information Commissioner

Response to the Consultation on the Children's Online Privacy Code

Technical Paper 2025.4

Submission to the Office of the Australian Information Commissioner

Response to the Consultation on the Children's Online Privacy Code

SUMMARY

This submission by the International Panel on the Information Environment (IPIE) sets out recommendations for the development of the Children's Online Privacy Code under Australia's Privacy Act 1988. The purpose of this submission is to offer guidance to policymakers on how to balance privacy protection with legitimate data access and use while protecting children from technology-facilitated child sexual exploitation and abuse (CSEA) and related privacy harms in digital environments.

IPIE recommendations are summarized as follows:

- **Recommendation 1**: The Code should adopt the broadest possible scope when determining which actors qualify as Australian Privacy Principles (APP) entities[1], to ensure technology-neutral and business model-agnostic coverage based on likelihood of access by children.

- **Recommendation 2**: The Code should ensure privacy protections do not impede legitimate child protection efforts, particularly in detecting, preventing and investigating technology-facilitated child sexual exploitation and abuse (CSEA), while supporting anonymized data-sharing for research and investigatory purposes.

- **Recommendation 3**: The Code should establish robust transparency and accountability mechanisms that require entities subject to the Australian Privacy Principles to demonstrate child protection effectiveness through verifiable evidence, external scrutiny, comprehensive impact assessments, and transparency about existing CSEA mitigation measures.

BACKGROUND

IPIE is an independent and global science organization providing scientific knowledge about the health of the world's information environment. Based in Switzerland, the IPIE offers policymakers, industry, and civil society actionable scientific assessments about threats to the information environment, including AI bias, algorithmic manipulation, and disinformation. IPIE is the only scientific body systematically organizing, evaluating, and elevating research with the broad aim of improving the global information environment. Hundreds of researchers worldwide contribute to the IPIE's activities.

---

[1] The Australian Office of the Australian Information Commissioner, in its issue paper on OAIC Children's Online Privacy Code defines APP entities as "any organisation or agency that is subject to the *Privacy Act 1988"*.

This submission draws primarily on an IPIE technical paper*, The role of technologies in facilitating child sexual exploitation and abuse: A mapping exercise,*[1] which comprehensively mapped how digital technologies enable child sexual exploitation and abuse across content, contact, conduct, and contract risks, identifying specific data variables and evidence sources that reveal patterns of technology-facilitated CSEA and the critical privacy governance gaps that enable such exploitation. The technical paper is available upon request from Prof. Philip Howard (philip.howard@ipie.info) or Prof. Selcan Kaynak (Selcan.Kaynak@ipie.info).

The submission also draws on existing UK and EU law, as well as scholarly publications.

IPIE RECOMMENDATIONS

Recommendation 1: The Code should adopt the broadest possible scope when determining APP entity inclusion, addressing the scope of services covered by the code and question (APP1).

IPIE advocates for the broadest possible scope of APP entity coverage by adopting a technology-neutral and business model-agnostic approach to defining entities in scope to capture those likely to be accessed by children. Definitions should therefore focus on the functionalities or capabilities that appeal to or are beneficial for children, and which expose children to risk, such as content recommendation, monetization of user-generated content, data profiling, or hosting user-to-user communications, rather than industry sector, contractual relationship with the user, or product type.[2]

The Code should also adopt the approach to inclusion recommended by the Age-Appropriate Design Code (UK), which is based on whether the entity is likely to be accessed by children or used by others in ways that involve processing children's personal data, rather than specific percentages of child users or categorical determinations based on service type. In an internal technical paper reviewing scientific and legal publications as well as legislative proceedings and court cases, the IPIE identified social media platforms, communication platforms (e.g., Discord), and gaming networks as channels through which perpetrators search for and gain access to potential child victims.[3] Furthermore, Internet Service Providers (ISPs) enable mass distribution of child sexual abuse material (CSAM). Perpetrators use GenAI applications to generate deep-fake pornography and CSAM, and financial platforms facilitate CSEA monetization, with perpetrators using this to pay for CSAM content.[4]

Given the wide range of potential services that could be involved in the processing and distribution of CSAM and the facilitation of CSEA, regulators should ensure that the definition of an APP entity in the scope of regulation covers all services that process or facilitate the processing of children's data, whether children directly engage with the services, or not.

Recommendation 2: The Code should ensure privacy protections do not impede legitimate child protection efforts, addressing the issues of anonymity and pseudonymity and collection of solicited personal information (APP 5 and APP6).

IPIE emphasizes that privacy codes should not curtail child protection efforts or create barriers to detecting, preventing and investigating technology-facilitated CSEA. While privacy rights are fundamental, they should be balanced against children's safety needs.

The double-edged nature of privacy features: Anonymized accounts and privacy-enhancing technologies present complex challenges for APP entities. Privacy-enhancing technology, such as end-to-end encryption, are critical for protecting children's privacy online, securing their communications from surveillance and unauthorized access. However, end-to-end encryption has been abused by perpetrators to hide their communication with victims, mitigate the risk of detection, and conceal their illegal activities.[5] Furthermore, privacy protections can impede necessary child protection measures. Technology used to conceal illegal activities (e.g., encryption, anonymization) or limit digital traces of these activities (e.g., live streaming) makes it difficult for technology companies to monitor and detect content and communication related to CSEA exchanged across networks and services.[6]

While such protections may impede certain child protection measures by limiting direct visibility into harmful interactions, a range of other data sources—including metadata, user interaction logs, platform moderation records, and network traffic—could be leveraged to support investigations and enhance child safety without undermining encryption. This is provided that the purpose of such data use is made clear to users.[7]

Moving beyond current age verification methods: Scientific research identifies varying degrees of the real-world effectiveness across age assurance and age verification technologies. Although technology advances have brought about improvements in some age assurance and verification methods, such as face analysis technology,[8] the effectiveness of the various age assurance and verification methods still varies.[9] APP entities should therefore not rely solely on age verification but should assess and anticipate the impacts of their products and services on children and their rights, referring to various forms of impact assessments, including data protection, algorithmic, human and child rights impact assessments, as appropriate.

Supporting legitimate data access while balancing privacy concerns: A balanced approach should offer children privacy protections while preventing the abuse of these same features by perpetrators seeking to exploit children. While protecting individual privacy, APP entities should support anonymized data-sharing for research and investigatory purposes to combat tech-facilitated CSEA. IPIE's research highlights that acquiring data pertaining to technology-facilitated CSEA remains challenging due to legal loopholes, opaque platform policies, pervasive encryption, and short data retention windows that block investigators and researchers.[10] Moreover, by the time law enforcement or researchers receive authorization to access these data, companies may have routinely erased communications and internet traffic data due to their storage capacity limitations.[11] To facilitate child protection efforts, APP entities should be

required to process and grant access to legitimate requests to access personal data for child protection purposes in a timely manner.

Recommendation 3: The Code should establish robust transparency and accountability mechanisms for APP entities, addressing access to personal information.

IPIE advocates for robust transparency and accountability mechanisms requiring APP entities to demonstrate their child protection efforts through verifiable evidence and external scrutiny.

Data-sharing for child protection: APP entities should support anonymized data-sharing that serves the collective benefit of child protection. They should enable researcher and agency access to anonymized data to investigate tech-facilitated CSEA while ensuring appropriate governance frameworks protect children's interests.

APP entities should ensure APP1 obligations are met—particularly when children are not the intended primary users—by enabling independent evaluation through comprehensive data-sharing and the possibility of cross-examination upon request.[12] Any analysis and testing that companies have conducted should be accompanied by publicly available raw data and background materials so that these company-provided results can be independently cross-examined. APP entities should maintain detailed records of both their test results and testing procedures so that the same tests can be run by others to verify company-provided results. This measure would ensure APP entities cannot simply self-report their effectiveness without external validation.

Impact assessment: APP entities should conduct comprehensive privacy impact assessments examining how their recommendation systems collect, process, and use children's personal data. These assessments must evaluate how the use of children's personal data in algorithmic systems may increase exposure to harmful content, facilitate inappropriate contacts, or elevate CSEA risks.

Relevant assessment data and protocols should be available to regulatory authorities and qualified researchers upon request. Such a privacy-focused transparency requirement would ensure that data provided by APP entities are subject to external validation, and that they provide quantitative data regarding the effectiveness of their data protection measures. This approach aligns with that of the EU Digital Services Act which requires platforms to conduct risk assessments concerning CSAM dissemination.[13]

Operational transparency: When collecting children's personal information, APP entities should ensure such collection is reasonably necessary for their functions. This standard should be interpreted on a case-by-case basis, with the operation and intended purpose of the entity's products or services determining what constitutes reasonable necessity. To ensure APP entities adhere to this standard, they should, when requested, disclose technical details about how their systems process individuals' data. This would enable robust cross-examination of their practices and verification that their data collection

processes align with legitimate operational needs and adheres to general privacy standards and specific protections for children's data.

‘Lawful’ and ‘fair’ data practices in the context of children’s personal information: APP entities should ensure compliance with relevant laws when collecting and processing data (‘lawful practices’). ‘Fair practice’ means collecting and processing data in ways consistent with what companies tell users (transparency) and in ways users, especially children, can reasonably expect. ’Fair’ should also include ensuring that outcomes of data processing are not exploitative: data practices must not result in children being profiled or exposed to CSAM material, through content or contact recommendation systems or targeted advertising.[14] Furthermore, APP entities should implement built-in friction for data-sharing, notifying children of data types being shared and offering them control functions to manage data sharing.

REFERENCES

[1] International Panel on the Information Environment. *The role of technologies in facilitating child sexual exploitation and abuse: A mapping exercise*. Technical Paper 2025.1. Zurich, Switzerland: IPIE.
[2] Ibid.
[3] Ibid.
[4] Idem, pp. 25–28.
[5] International Panel on the Information Environment. *The role of technologies in facilitating child sexual exploitation and abuse: A mapping exercise*. Technical Paper 2025.1. Zurich, Switzerland: IPIE.
[6] Idem, p.33.
[7] International Panel on the Information Environment. *The role of technologies in facilitating child sexual exploitation and abuse: A mapping exercise*. Technical Paper 2025.1. Zurich, Switzerland: IPIE.
[8] P. J. Grother, M. L. Ngan, J. Yang, G. W. Quinn, and A. Hom, ‘Face analysis technology evaluation: age estimation and verification’, National Institute of Standards and Technology, Gaithersburg, MD, May 2024. doi: 10.6028/nist.ir.8525.
[9] M. Sas and M. Jan Tobias, ‘Trustworthy Age Assurance? A risk-based evaluation of available and upcoming age assurance technologies from a fundamental rights perspective’, The Greens/EFA in the European Parliament, 2024. [Online]. Available: https://www.greens-efa.eu/files/assets/docs/age_assurance_v2.1.pdf
[10] International Panel on the Information Environment. *The role of technologies in facilitating child sexual exploitation and abuse: A mapping exercise*. Technical Paper 2025.1. Zurich, Switzerland: IPIE, p.33.
[11] Ibid.
[12] Idem, p.10.
[13] European Parliament and Council. *Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act).* 2022. Brussels, Belgium: Official Journal of the European Union. Available: https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng
[14] International Panel on the Information Environment. *The role of technologies in facilitating child sexual exploitation and abuse: A mapping exercise*. Technical Paper 2025.1. Zurich, Switzerland: IPIE.

International Panel on the Information Environment

Seefeldstrasse 123
P.O. Box 8034 Zurich
Switzerland