

Privacy 108 Submission to the Exposure Draft of the Children's Online Privacy Code (COPC)

Thank you for the opportunity to provide a submission in response to the Children's Online Privacy Code Exposure Draft (**Exposure Draft**).

Privacy 108 is a specialist privacy consultancy and law firm with expertise in information privacy law, AI governance, data security, and technology regulation. We work across the public and private sectors and have advised State and Local government agencies (including agencies responsible for handling children's personal information on a State-wide basis), ASX-listed companies, not-for-profits, healthcare providers, and educational institutions.

We welcome the release of the Exposure Draft and thank the OAIC for the consultative approach that has been adopted to date. Overall, Privacy 108 is highly supportive of the draft COPC, which represents a significant and welcome enhancement of Australia's privacy framework. In our view, the COPC has the potential to deliver a meaningful and enduring uplift in the protection of children in online environments.

This submission proceeds by providing feedback on the following aspects of the Exposure Draft:

1. Scope of application
2. Age assurance
3. Privacy protections
4. Privacy risk management measures and Privacy Impact Assessments

I. Scope of application

The scope of the application of the COPC is a critical threshold issue. It determines which entities are subject to the COPC's protections and, consequently, whether children will meaningfully benefit from the enhanced privacy safeguards it introduces. Ensuring that the scope is clear, comprehensive and aligned with privacy risks is therefore fundamental to the effectiveness of the COPC.

Under the *Privacy Act 1988* (Cth), APP entities that meet the following criteria will be automatically bound by the COPC:¹

- a) the entity is a provider of a social media service, relevant electronic service or designated internet service (all within the meaning of the *Online Safety Act 2021* (Cth))²;
- b) the service is likely to be accessed by children; and
- c) the entity is not providing a health service.

¹ *Privacy Act 1988* (Cth) s 26GC(5)(a). This was introduced by the *Privacy and Other Legislation Amendment Act 2024* (Cth).

² 'Relevant electronic services' generally consist of online services that facilitate communication between users (e.g. messaging apps, email, video calling platforms, online games with chat). 'Designated internet service' is defined broadly to include online services that allow users to access or receive material over the internet (e.g. cloud storage, websites that let users receive/access content, streaming platforms, consumer IoT devices). For further details, refer to *Online Safety Act 2021* (Cth) ss 13A and 14.

The OAIC is also able to prescribe additional entities that will be bound by the Code.³ To this end, Section 5 of the Exposure Draft proposes to also capture services that are ‘**primarily concerned with the activities of children**.’⁴

We support the OAIC’s policy intent to capture services that are ‘not made for children and not used by children’ but nevertheless handle large volumes of personal information about children.⁵ For example, the OAIC states this could include apps that track early childhood development, family photo sharing apps, online school management systems that monitor student performance, and internet-connected baby monitors.

However, as currently drafted, the scope may not capture certain categories of entities that present comparable, or in some cases greater, privacy risks to children. Some entities are likely to fall outside the scope of the COPC because their services are not ‘accessed by children’ or ‘primarily concerned with the activities of children’ specifically, even though they handle large volumes of sensitive personal information about children or engage in pervasive monitoring or profiling practices.

This includes, for example:

- Operators of **one-to-many facial recognition or biometric identification systems**⁶ that collect the personal information of individuals from public or semi-public spaces, including children, but are not ‘*primarily concerned with the activities of children*’, and
- **Data brokers** that collect, aggregate, analyse or disclose personal information relating to children⁷ but again are not *primarily concerned with children specifically* (as compared to the general public) and whose services are not ‘accessed’ by children.

If left outside of the COPC, these activities would not be subject to the COPC’s enhanced protections, creating a material gap in the regulatory framework.

We therefore submit that the scope of the COPC should be expanded to capture high-risk processing of children’s personal information, including where a service may not be *primarily* directed towards, or accessed by children. A **risk-based extension of scope** would better align the application of the COPC with the harms it is intended to address.

The OAIC could prescribe the following types of online services within Section 5, in addition to entities that are ‘primarily concerned with the activities of children’:

- Services that collect, use or disclose children’s sensitive information on a large scale; and
- Services that profile or monitor children, in a manner that is likely to result in a high risk to their privacy.

³ Privacy Act 1988 s 26GC(5)(b).

⁴ Exposure Draft s 5. Note that the entity will also have to fall within the definition of a social media service, relevant electronic service or designated internet service under the *Online Safety Act 2021* and must not be providing a health service.

⁵ OAIC, *Extended Guide to the Draft Children’s Online Privacy Code*, 7; OAIC, *Exposure Draft Explanatory Statement*, 5.

⁶ For the difference between ‘one-to-many’ facial identification and ‘one-to-one’ facial verification technologies, refer to Australian Human Rights Commission, [Human Rights and Technology Final Report](#), page 113 and UTS HTI, [Facial Recognition Technology: Towards a Model Law](#), page 15. However, there may be instances in which the use of biometric identification systems may be proportionate, such as for law enforcement purposes (with strict safeguards) or for the identification of missing persons.

⁷ For example, Reset Tech Australia’s [Australians for sale: targeted advertising, data brokering, and consumer manipulation](#) highlights ‘audience segments’ (or characteristics) held by data brokers about Australian children. See pages 39-45.

To promote regulatory certainty, the OAIC could provide guidance on the interpretation of key concepts such as ‘large scale’, ‘profiling’ and ‘monitoring’. The concept of ‘large scale processing’ is used within the GDPR to delineate certain forms of high-risk processing activities⁸ and the OAIC could refer to guidance issued by the UK Information Commissioner’s Office⁹ and European Commission¹⁰ to further clarify this concept. The OAIC could also refer to overseas data protection laws to inform definitions of ‘profiling’¹¹ and ‘monitoring’¹² for the purpose of extending the scope of the COPC.

If it were to adopt our recommendation, the OAIC would need to consider whether facial recognition services and data brokers would fall within the existing definitions under the Online Safety Act, including whether these entities fall within the concept of a ‘designated internet service’, or whether additional clarification is required to support their inclusion within the Code’s scope. As with the existing approach in Section 5 of the Exposure Draft, entities that provide a health service could remain exempted.

Recommendation 1 – Expand the scope of the COPC

In addition to services that are ‘primarily concerned with the activities of children’, the OAIC should also bring the following services within scope of the COPC under Section 5 of the Exposure Draft:

- Services that collect, use or disclose children’s sensitive information on a large scale, and
- Services that profile or monitor children, in a manner that is likely to result in a high risk to their privacy.

This would ensure that entities that handle large volumes of highly sensitive personal information about children or otherwise track or profile children are within scope, such as one-to-many facial recognition systems or data brokers.

2. Age assurance

Children’s online privacy codes in overseas jurisdictions ordinarily feature rules in relation to age assurance to guide online services about the steps they must practically take (if any) to identify the users that will receive the benefit of additional privacy protections.

Section 8 of the Exposure Draft provides that:

- Entities must take **reasonable steps** in the circumstances to ascertain end-users’ age
- In determining what steps are reasonable, entities must consider the **risk of harm** that may arise from handling the individual’s personal information through their services

⁸ Article 35(3) GDPR provides that Data Protection Impact Assessments (DPIAs) are required for ‘processing on a large scale of special categories of data’, among other circumstances. See also, Recital 91 GDPR.

⁹ See UK ICO, [When do we need to do a DPIA?](#)

¹⁰ See, European Commission Article 29 Data Protection Working Party, [Guidelines on Data Protection Impact Assessment \(DPIA\) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679](#), page 10.

¹¹ The GDPR and Californian Age-Appropriate Design Code define profiling as ‘any form of automated processing of personal data consisting of the use of personal data to evaluate certain aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.’

¹² Refer to GDPR Recital 24 and European Commission Article 29 Data Protection Working Party, [Guidelines on Data Protection Impact Assessment \(DPIA\) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679](#), page 9.

- Entities should **destroy sensitive information** as soon as practicable after ascertaining the user's age, and
- Entities do not need to perform age assurance if they **apply the protections in the Code to all users of the service**, regardless of age.

This risk-based approach is broadly consistent with children's codes in overseas jurisdictions such as the UK,¹³ California¹⁴ and Ireland.¹⁵ It encapsulates a range of possible age assurance techniques that offer varying degrees of certainty, including user self-declarations, parental attestations, AI-enabled age estimation or age inference techniques, and age verification.

These methods also present varying degrees of privacy risk to end-users. Methods that involve the collection of identity documents, financial information or biometric data for age verification purposes present a particularly high risk to data subjects due to the potential for these kinds of data to be compromised in a data breach, which may lead to downstream risks of identity theft and financial harm. The potential privacy risk associated with age assurance techniques arises not only from whether information is classified as 'sensitive information' under the Privacy Act, but also from the nature and potential misuse of the information collected.

Considering the potential risks associated with ID-based age verification, we submit that Section 8(4) of the Exposure Draft should not be limited to the destruction of *sensitive information* used for age assurance purposes. This documentation (i.e. identity documents or financial information) generally falls outside the definition of sensitive information in the *Privacy Act* and could be collected by certain online services to perform age assurance in high-risk circumstances.¹⁶

We suggest that section 8(4) should be expanded to require the destruction of *personal information* used for age assurance purposes as soon as practicable.¹⁷ This would also align more closely with the approach taken under the *Social Media Minimum Age Act*, which requires that entities who hold personal information for age assurance purposes destroy the information after that purpose has been met.¹⁸

Recommendation 2 – Require the destruction of personal information used for age assurance purposes

Section 8(4) of the Exposure Draft should be amended to require that entities destroy *personal*

¹³ The UK ICO's [Age-Appropriate Design Code](#) requires entities to '[t]ake a risk-based approach to recognising the age of individual users and ensure you effectively apply the standards in this code to child users. Either establish age with a level of certainty that is appropriate to the risks to the rights and freedoms of children that arise from your data processing, or apply the standards in this code to all your users instead.'

¹⁴ Under California's [Age-Appropriate Design Code](#), entities must '[e]stimate the age of child users with a reasonable level of certainty appropriate to the risks that arise from the data management practices of the business or apply the privacy and data protections afforded to children to all consumers.'

¹⁵ Ireland's [Fundamentals for a Child-Oriented Approach to Data Processing](#) states that online services should 'provide a "floor" of protection for all users, unless they take a risk-based approach to verifying the age of their users so that the protections set out in the Fundamentals are applied to all processing of children's data'.

¹⁶ See for example, BBC News, [ID photos of 70,000 users may have been leaked, Discord says](#).

¹⁷ For example, the Californian Age-Appropriate Design Code prohibits entities from 'using any personal information collected to estimate age or age range for any other purpose or retain that personal information longer than necessary to estimate age', see California Age-Appropriate Design Code §1798.99.31(b)(8).

¹⁸ *Online Safety Amendment (Social Media Minimum Age) Act 2024* (Cth), s 63F(3). See also, eSafety Commissioner, *Social Media Minimum Age Regulatory Guidance*, 25, which states that 'eSafety does not expect providers to retain personal information as a record of individual age checks.' Refer also to OAIC, *Privacy Guidance on Part 4A (Social Media Minimum Age) of the Online Safety Act 2021*, 19-25.

information used for age assurance purposes as soon as practicable. The draft provision is currently limited to requiring the destruction of *sensitive information*.

This would ensure that high-risk types of personal information that fall outside the definition of sensitive information (e.g. ID documents, credit cards) and which are collected by entities for age assurance purposes are subject to the more stringent destruction requirements in section 8(4) of the COPC. It would also ensure alignment with the age assurance controls in Australia's online safety regime.

3. Privacy protections

The Exposure Draft proposes to introduce a range of new privacy protections for children in online settings. Privacy 108 is supportive of the following requirements:

- That entities implement technical and organisational measures to ensure that they only collect personal information that is **strictly necessary** to provide the service, by default
- Collections, uses and disclosures must be consistent with the **best interests of the child**
- **Consent** must be voluntary, informed, current, specific, unambiguous and easy to withdraw
- Entities must provide **age-appropriate privacy policies and collection notices**
- Entities must provide **information about how they handle the child's personal information** (e.g. categories, source of personal information, etc.), on request, and
- Obligation to **destroy personal information** about a child, on request.

a) *Best interests of the child*

Privacy 108 is strongly supportive of the requirement for collections, uses and disclosures to be consistent with the best interests of the child.¹⁹ This will represent a significant uplift of privacy standards as compared to APP 3 and APP 6 and will ensure that children's wellbeing is placed at the centre of decision-making across the information lifecycle. It will allow for holistic, child-centered assessments of personal information handling practices that consider broader child rights and developmental considerations. The proposed test will play a critical role in ensuring that online services are designed in a manner that meaningfully protects children and would be consistent with leading overseas children's privacy codes.²⁰

The broad framing of the best interests test will enable it to apply flexibly across different business models and personal information handling practices. However, this will also require regulatory guidance from the OAIC to help industry understand how the test will apply in practice in different circumstances. For example, the UK Age-Appropriate Design Code provides guidance about how the best interests principle may apply with respect to specific practices such as geolocation tracking, data sharing, default settings,²¹ as well as potential conflicts between commercial interests and the best interests of the child.²² Similar guidance from the OAIC will be

¹⁹ Exposure Draft ss 10-11.

²⁰ See e.g., UK Age-Appropriate Design Code, California's Age-Appropriate Design Code and Ireland's Fundamentals for a Child-Oriented Approach to Data Processing.

²¹ UK Age Appropriate Design Code, [Profiling](#), [Geolocation](#), [Data Sharing](#), [Default Settings](#).

²² For example, the UK Age-Appropriate Design Code and Californian Age-Appropriate Design Code state that where a conflict arises between commercial interests and the best interests of children, the child's wellbeing and right to privacy should be prioritized. See Californian Age-Appropriate Design Code §1798.99.29, UK Age-Appropriate Design Code, [Best Interests of the Child](#).

critical to support industry compliance with the best interests test. We note that some of these matters have already been explored in the Exposure Draft Explanatory Statement.

Recommendation 3 – Regulatory guidance on the best interests of the child

During implementation, the OAIC should prepare further regulatory guidance on the application of the ‘best interests of the child’ test, including how the test may apply to specific practices such as the handling of geolocation data, data sharing, the application of default settings and the management of conflicts between commercial interests and the best interests of the child.

This guidance will be crucial to support industry compliance and understanding as to how the test will apply in practice.

With respect to uses and disclosures specifically, section 11(1) of the Exposure Draft currently provides that ‘[i]n complying with Australian Privacy Principle 6.1, an entity must not use or disclose personal information about a child unless:

- a) the child has **consented** to the use or disclosure of the information; and
- b) the use or disclosure of the information is consistent with the **best interests of the child.**

The current framing of this provision contains some ambiguity as to whether these conditions need to be met **only for secondary purposes, or also for primary purposes**. We submit that entities should be required to meet the best interests test for *all* uses and disclosures, regardless of whether it is for a primary or secondary purpose. This would provide a baseline level of assurance that the wellbeing of children has been considered prior to an entity engaging in a use or disclosure.

However, the OAIC may wish to consider the potential risk of consent fatigue should entities be required to obtain consent for primary purposes, which may potentially lead to parents and children being overwhelmed by a large volume of consent requests and not being able to effectively engage with those consents.²³ The experience of cookie consent requests under Europe’s ePrivacy Directive may be instructive in this regard.²⁴

Recommendation 4 – Clarify requirements for uses and disclosures

The Exposure Draft should be clarified to indicate whether the requirements of section 11(1) apply to primary purposes as well as secondary purposes. We submit that entities should be required to meet the ‘best interest of the child’ test for all uses and disclosures of children’s personal information (regardless of whether it is for a primary or secondary purpose).

However, the OAIC should proceed cautiously before requiring consent for primary purposes due to the potential risks of consent fatigue and reduced effectiveness of consent mechanisms.

²³ See, Daniel Solove, ‘Privacy Self-Management and the Consent Dilemma’ (2013) 126 *Harvard Law Review* 1880.

²⁴ In the European context, the consent requirements of the ePrivacy Directive led to individuals receiving a warning message about the use of cookies on almost every website, which arguably undermined the efficacy of the law. See, European Commission, *ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation* (31 January 2015) page 12; European Commission, *Synopsis Report of the Public Consultation on the Evaluation and Review of the ePrivacy Directive* (19 December 2016) page 2.

b) Prohibiting harmful practices

Privacy 108 submits that the draft COPC should clearly prohibit certain personal information handling practices that are harmful and would never be regarded as being in the best interests of the child. For example, these practices could include:

- The profiling of children for commercial purposes, particularly systems that infer sensitive information, or the vulnerabilities, emotions or personality characteristics of a child²⁵
- The sale or sharing of children's personal information²⁶ for a commercial benefit
- The collection, use or disclosure of children's personal information for inclusion in one-to-many facial recognition or biometric identification systems, except for law enforcement purposes or for identifying missing persons,²⁷ and
- Targeted advertising that is based on the profiling of a child, where the service is aware with reasonable certainty that the end-user is a child.²⁸

There is precedent in international regulatory frameworks for expressly prohibiting harmful data practices, including under the EU AI Act, Digital Services Act and Californian Age-Appropriate Design Code.²⁹ Additionally, the United Nations' *General Comment No. 25 on Children's Rights in Relation to the Digital Environment* recommends the prohibition of:

*'...the profiling or targeting of children of any age for commercial purposes on the basis of a digital record of their actual or inferred characteristics, including group or collective data, targeting by association or affinity profiling. Practices that rely on neuromarketing, emotional analytics, immersive advertising and advertising in virtual and augmented reality environments to promote products applications and services should also be prohibited from engagement directly or indirectly with children.'*³⁰

Aligning protections for Australian children with jurisdictions such as Europe and California would support consistency with emerging international standards.

Furthermore, these express prohibitions would provide clarity to industry as to which practices are not permissible, which enhances certainty and would support more consistent interpretation of the COPC across the sector. From a regulatory perspective, it may also reduce regulatory costs for the OAIC to have the option of enforcing these more straightforward prohibitions in certain circumstances, in place of the more flexible, principles-based best interests test (which will require a nuanced, case-by-case assessment).

Recommendation 5 – Prohibit harmful personal information handling practices

The COPC should prohibit certain personal information handling practices that are generally harmful and are unlikely to be consistent with the best interests of the child:

- The profiling of children for commercial purposes in a manner that involves the inference of sensitive information, or the vulnerabilities, emotions or personality

²⁵ See relatedly, United Nations Committee on the Rights of the Child, *General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment*, page 7 ('**General Comment No. 25**'), California Age-Appropriate Design Code §1798.99.31(b)(2) and EU AI Act, Articles 5(1)(b), (c), (f), (g). Refer to Footnote 11 above for the definitions of 'profiling' adopted in the GDPR and California AADC.

²⁶ See relatedly, California Age-Appropriate Design Code §1798.99.31(b)(3), (5).

²⁷ See relatedly, EU AI Act, Articles 5(1)(e), (g), (h) and General Comment No. 25, page 7.

²⁸ See relatedly, EU Digital Services Act, Article 28(2).

²⁹ Refer to Footnotes 25-28 above.

³⁰ General Comment No. 25, page 7.

characteristics of a child

- The sale or sharing of children's personal information for commercial benefit
- The collection, use or disclosure of children's personal information for inclusion in one-to-many facial recognition or biometric identification systems, except where strictly necessary for law enforcement purposes or for identifying missing persons, and
- Targeted advertising that is based on the profiling of a child, where the service is aware with reasonable certainty that the end-user is a child.

4. Privacy risk management measures and Privacy Impact Assessments

The Exposure Draft proposes specific privacy risk management measures for online services that are bound by the COPC, including that:

- **Section 25** – Entities must **annually review** and update their practices, procedures and systems to ensure that they comply with the Australian Privacy Principles and the COPC. Entities must keep records of these reviews and provide these records to the OAIC, on request.
- **Sections 38 and 39** – Entities must perform a **Privacy Impact Assessment (PIA)** before providing a new service to children or adopting any new or changed ways of handling personal information that are likely to have a significant impact on the privacy of children. Entities must maintain a register of PIAs that they have conducted, which must be published online.
- **Section 40** – Entities must provide **education and training** about the handling of children's personal information for staff.

Privacy 108 strongly supports these proposed obligations. Collectively, these measures will require entities to take a proactive and systematic approach to identifying, assessing and managing privacy risks, and will require them to embed the consideration of children's privacy early in the design and ongoing operation of their online services. This is likely to translate into more consistent and robust protection for children and will ensure that risks are addressed before they materialise.

PIAs are a particularly important accountability mechanism, as they require entities to systematically identify and assess privacy risks before they arise, and to document the reasoning underpinning their decisions. This promotes more thoughtful and responsible data handling practices, ultimately leading to services that better reflect community expectations and safeguard the interests of children.

We support the prescriptive approach that has been taken in section 38(2) of the Exposure Draft, which lists the matters that a PIA must include for the purposes of the COPC:

- a) a description of the nature, scope, context, flow and purposes of the handling of children's personal information
- b) an explanation as to why the collection of children's personal information is strictly necessary to provide the service or activity
- c) an explanation as to how the collection of children's personal information is done by lawful and fair means
- d) an assessment of whether the handling of children's personal information is consistent with the best interests of the child and a record of this assessment, including the reasoning on which the assessment is based

- e) specific information about how the entity complies with this Code and the Act, and
- f) an assessment of the risk of harm to, and the potential impact on, children resulting from the handling of their personal information.

This provision provides clarity to entities as to the OAIC's expectations regarding the scope and content of PIAs in this context and will promote greater consistency in how privacy risks are assessed across online services. Additionally, by requiring entities to document their reasoning (particularly in relation to the "best interests of the child" test), this provision will encourage more rigorous, evidence-based assessments rather than superficial or 'box-ticking' exercises.

Conclusion

Privacy 108 strongly supports the introduction of the COPC and the significant uplift in protections it represents for children in online environments. The measures proposed in the Exposure Draft, particularly the 'best interests of the child' test and enhanced accountability mechanisms, will play a critical role in improving privacy outcomes for children.

More broadly, Privacy 108 is of the strong view that the remaining proposals from the Attorney-General's Department's *Privacy Act Review Report* should be progressed by Government to provide holistic privacy protections for all Australians, as well as to improve trust in the digital economy. To this end, we are also supportive of the OAIC's continued advocacy regarding the progression of these reforms.

We would be pleased to meet with the OAIC to provide you with further details on any of our comments or recommendations in this submission.

Thank you for your consideration.

Privacy 108