

Australia's Draft Children's Online Privacy Code

Submission by 5Rights Foundation – June 2026

From the moment a child opens an application, plays a game, or visits a website, data is being collected, used, stored, and inferred about them. This directly drives many norms of the digital world and shapes both children's digital experiences and real-life outcomes.

The latest Global Privacy Enforcement Network Sweep found that children in Australia and across the world face more pervasive privacy risks today than they did in 2015.¹ As technology increasingly mediates all aspects of children's lives, tech companies have made their participation in the digital world conditional on surrendering to invasive practices intentionally designed to harvest, share, and sell their data for profit, build profiles and predict behaviour. Yet, the value of children's data and the full extent of this commercial exploitation remain largely opaque to most users and almost entirely invisible to all children.

Five years ago, the adoption of UNCRC General comment No. 25 offered the world a roadmap to realise in the digital world the rights enshrined in the most widely ratified human rights treaty in history: the UN Convention on the Rights of the Child.

Since then, best practices enshrining age-appropriate design standards and holding tech companies accountable for respecting children's rights by design and default have emerged across every continent.² When regulation – such as the UK's Age-Appropriate Design Code – requires tech companies to demonstrate respect for children's privacy and safety before reaching the market, evidence shows that they increase privacy protections in children's default settings, redesign recommender systems, and restrict targeted advertising to children.³ Conversely, in the absence of robust regulation and enforcement, tech companies continue to shift responsibility to users and provide unequal safeguards across jurisdictions – including in Australia.⁴

In the face of unprecedented data collection, sharing and monetisation, we welcome the OAIC's leadership in developing a draft Children's Online Privacy Code that extends best practice protections to all children in Australia. Robustly implementing the standards set out in UNCRC General comment No. 25, the draft Code represents a critical step towards establishing minimum rules for rights-respecting innovation and holding tech companies accountable for respecting children's rights and best interests – by design and default – so that children can enjoy the benefits of technology without being subjected to commercial surveillance, exploitation, and manipulation

¹ 5Rights, [Children face greater privacy risks today than a decade ago and tech companies are to blame](#).

² 5Rights, [Building a digital environment designed with children in mind: An international best practices blueprint](#). / Ringmar Sylwander, [Mapping the global impact of UNCRC General comment No. 25 on children's rights in the digital environment](#).

³ Wood, [Impact of regulation on children's digital lives](#).

⁴ Wood, [Impact of regulation of children's digital lives - Phase II](#). / Béjar et al., [Teen Accounts, Broken Promises: How Instagram is Failing to Protect Minors](#). / Fairplay, [Global platforms, partial protections: Design discriminations on social media platforms](#).

We particularly welcome:

The draft Code includes crucial elements to implement the standards set out in the UN Convention on the Rights of the Child and its accompanying General comment No. 25.

- The scope covers all services likely to be accessed by children and expands international best practice by also including services 'primarily concerned with the activities of children', ensuring children's privacy is protected on services that are likely to impact their rights indirectly.⁵ (§§ 5 & 7)
- The prioritisation of children's rights above commercial interests, by prohibiting the collection, use, and disclosure of children's personal information unless consistent with the best interests of the child and the requirement that tech companies justify this consideration through privacy impact assessments. Requiring high privacy by design and by default also alleviates the challenges associated with obtaining and managing informed (parental) consent and ensures that children's data is protected regardless of their abilities to grasp the nuances of data privacy.⁶ (§§ 10, 11, & 38)
- The placement of responsibility on tech companies to assess their impact on children's privacy upstream by mandating privacy impacts assessments before services reach the market.⁷ (§ 38)
- The enshrining of data minimisation and purpose limitation by requiring that tech companies only collect, use, and disclose children's personal information where strictly necessary – and demands that tech companies justify this strict necessity through privacy impact assessments.⁸ (§§ 9 & 38)
- The prohibition of opaque and deceptive practices to manipulate children into consenting to the collection, use, or disclosure of their data.⁹ (§§ 14, 15, 18, 19, & 21)
- The recognition that age assurance is not a silver bullet, only mandating privacy-preserving age assurance where services do not offer rights-respecting and age-appropriate digital experiences to all users by design and default.¹⁰ (§ 8)
- The correction of the power imbalance cultivated by tech companies, returning agency to children through control over data collection, use, and disclosure; age-appropriate published terms; and mechanisms to access, correct, and destroy personal information.¹¹ (§§ 9, 23, 24, 30, 31, & 32)

We recommend:

To ensure the draft Code fully implements the standards set out in UNCRC General comment No. 25 and builds on international best practices – as outlined in 5Rights' [Approaches to Children's Data Protection](#) – certain provisions should be strengthened.

- SCOPE (§§ 5 & 7): The scope could be further broadened to cover services likely to impact children indirectly, beyond those primarily concerned with the activities

⁵ UNCRC General comment No. 25, para. 4.

⁶ UNCRC General comment No. 25, para. 110.

⁷ UNCRC General comment No. 25, para. 38.

⁸ UNCRC General comment No. 25, paras. 69 & 73.

⁹ UNCRC General comment No. 25, paras. 70, 75, and 77.

¹⁰ 5Rights, [Building a digital environment designed with children in mind: An international best practices blueprint](#), pp. 38-40. / 5Rights, [But how do they know it's a child?](#)

¹¹ UNCRC General comment No. 25, paras. 39 & 70.

of children.¹² This would notably encompass AI systems which are trained on children's data, shape children's experiences, and generate outcomes or influence decisions likely to impact children – as well as Internet of Things devices which routinely collect and process information about unsuspecting bystanders with no relationship to the provider.¹³

- **PRIVACY IMPACT ASSESSMENTS (§ 38):** In addition to assessing their impact on children's privacy, tech companies must be required to mitigate risks to children likely to access or be impacted by their products, services, and features. PIAs must also be conducted when the Code comes into effect and periodically, not just when new products, services, or features are released.¹⁴
- **GEOLOCATION (§ 33):** It is insufficient for tech companies to only notify children when other users can monitor their geolocation. Geolocation settings must be turned off by default, unless a compelling reason that considers the best interests of the child requires otherwise. When location tracking is active, services must provide a clear, visible indicator for children. Any option making a child's location visible to others must automatically reset back to 'off' at the end of each session.¹⁵
- **DATA SUBJECT RIGHTS (§§ 30-32):** In addition to providing age-appropriate responses, mechanisms to request access, correction, and destruction of children's personal information must themselves be age-appropriate, accessible, and effective.¹⁶

¹² [UNCRC General comment No. 25](#), para. 4.

¹³ 5Rights, [Children & AI Design Code](#). / Business at OECD & United States Council for International Business Foundation, [Privacy, Immersive Technologies and the Metaverse](#).

¹⁴ [UNCRC General comment No. 25](#), paras. 23 and 38. For guidance, see UNICEF, [Assessing child rights impacts in relation to the digital environment](#).

¹⁵ [UNCRC General comment No. 25](#), paras. 40, 68, and 88.

¹⁶ [UNCRC General comment No. 25](#), para. 72.