Kim Ringmar Sylwander Sonia Livingstone August 20th, 2025

How can Australia's upcoming Children's Online Privacy Code learn from the UNCRC's General comment No. 25

As Australia's Information Commissioner develops a Children's Online Privacy Code, LSE's Kim Sylwander and Professor Sonia Livingstone explain the key points they made in their submission to the consultation on the Code, on behalf of the Digital Futures for Children centre and 5Rights.

Children's lives are increasingly shaped by the ways their data are collected, analysed and shared. Their online activities, emotional cues, interests, vulnerabilities, and behaviours may be recorded and inferences drawn about them. Yet many of the systems that extract value from children's data remain hidden from view, seemingly out of regulatory scope.

Australia, having ratified the UN Convention on the Rights of the Child (UNCRC), is legally bound to respect, protect and fulfil children's rights in all settings. General comment No. 25, adopted in 2021 by the UN Committee on the Rights of the Child, affirms that children's rights apply fully in relation to the digital environment. Its longest section concerns privacy, as befits today's datafied society, because "Privacy is vital to children's agency, dignity and safety and for the exercise of their rights" (para 67). Global Kids Online research shows that Australian children benefit in many ways from internet access, but also encounter a range of risks, and these are intensified for Aboriginal and Torres Strait Islander children.

A new children's online privacy code for Australia

Australia's Privacy and Other Legislation Amendment Act 2024 mandated the Office of the Australian Information Commissioner (OAIC) to develop a Children's Online Privacy Code. The Digital Futures for Children centre with 5Rights Foundation responded to the OAIC consultation in July 2025 to support the introduction of the Code. All our work is guided by the insights of General comment No. 25 and the importance of translating these into national law or other effective measures. We urged a rights-based approach that places children's rights above commercial interests for any service likely to be accessed by children (para 67, 68).

To the OAIC, we advocated that companies should carry out Child Rights Impact Assessments (CRIA) or, at a minimum, Data Protection (or Privacy) Impact Assessments when their services impact on children's data and rights, thus enabling organisations to anticipate and mitigate any negative impacts of their data processing, and children to correct or delete their data and claim remedy if needed. Our submission also stressed the need for clear, accessible communication: children must be able to understand what data is collected, how it is used, and what choices they have. Now that data fuels not only the attention economy but also its automation, we recommended the organisational practices set out in 5Rights' Children & AI Design Code.

Learning from General comment No. 25 on children's rights in the digital environment

If designed with ambition and enforced with care, Australia can deliver real protections for children online, now and into the future. But this will not be easy. The OAIC consultation asked many challenging questions which we sought to answer as follows:

1. ***What threshold should determine when a service is considered 'likely to be accessed by children'?*** According to General comment No. 25, any digital environment that intentionally targets, attracts, or is regularly used by children, whether directly or indirectly, should be considered "likely to be accessed" by children (paras. 74, 76). This includes not only platforms designed for children, but also those where children are known to be present, even if not the primary audience. It also includes commercial services used in public settings such as schools. Our research has found that while EdTech companies may claim to be merely the data processor, their actions are of such complexity and opacity that they constitute the data controller. This has led to difficulties regarding the scope of the Age Appropriate Design Code in the UK, so Australia is well advised to anticipate and resolve these.

- ***What role, if any, should age gating or other access control mechanisms play in meeting obligations under the Code?*** General comment no. 25 warns that overly restrictive or poorly implemented age verification can limit children's access to beneficial services, or compel them to misrepresent their age (para. 76). Research shows that children can circumnavigate poorly enforced age testing mechanisms. Age assurance should be proportionate, privacy-respecting, rights-respecting and not intrusive. Note further that the language of "age assurance" is preferred over age gating. The IEEE 2089.1-2024 Standard for Online Age Verification establishes a framework for rights-respecting age assurance systems, building on 5Rights' resource 'But how do they know it's a child?'

- ***Would age-based guidance help tailor protections and interfaces appropriately and effectively?*** Research consistently shows that children's understanding and needs vary by age but children do not fall neatly into fixed age categories, and even within a single age group there can be wide variation. Developmental psychology has moved beyond rigid "ages and stages" models but it also recognises that a five-year-old and a fifteen-year-old are not equivalent, as does the UNCRC's concept of evolving capacities. While children's specific needs, understandings, and circumstances will always matter, research supports some broad-brush age-specific provision, as since implemented by the UK's data protection and communications regulators.

- ***What does 'lawful 'and 'fair' mean in the context of children's personal information?*** For children, *lawful* means that data processing must be grounded in law and serve a legitimate purpose (para. 69). *Fair* means that it respects children's agency, dignity, and evolving capacities, and avoids any form of exploitation or harm (para. 67). As children may not fully understand how their data is being used, *fairness* requires transparency, the use of child-friendly language, and stronger safeguards in design and implementation. Practices such as routine or indiscriminate surveillance (para.75), opaque automated decision-making, or data use without clear benefit to the child are not fair, even if technically legal (paras. 68, 75). Genuine consent must be informed, freely given, and obtained – not assumed – before data is processed (para. 71). Servies should also respect the right to anonymity where appropriate, while ensuring safeguards against misuse (para. 77).

- ***What secondary uses or disclosures of personal information could be reasonably expected by children?*** Children's expectations of how their data might be reused or shared will vary based on age, maturity, and digital literacy (General comment No. 25, paras. 71, 76).

Reasonable expectations might include:

- Sharing relevant school data with a new educational institution (e.g. primary to secondary school) (para. 73)
- Sharing health data with medical professionals to ensure continuity of care
- Use of anonymised data for research, where there is no risk of identification.

However, children do not reasonably expect their data to be reused for:

- Commercial profiling, behavioural targeting, or advertising (para. 68)
- Unexplained cross-platform sharing
- Unauthorised use in predictive or recommender systems or AI model training
- Secondary use of children's data without clear and explicit consent

Further, research shows that:

- Privacy policies of products used by children are generally far from 'child-friendly' or accessible, including for required EdTech – this renders 'consent' meaningless and undermines fairness and remedy
- Research reveals children's deep concerns about unnecessary data collection – they describe it as "creepy" or "scary" or "none of their business"
- Fewer than one in ten UK 6-17 year olds thought it acceptable for the apps they used at school 'to share information about you and your classmates with other companies'
- Forty five percent of UK children aged 10-17 called for more digital products and services without advertising, suggesting it is not a 'reasonable expectation' that children's personal information can be used for direct marketing purposes.

Looking forward

In the UK, and a growing number of other countries, the right to privacy is encoded in an Age Appropriate Design Code (AADC, see the data protection authority's "Children's Code"), this triggering real-world protections for children. Relatedly, the European Digital Services Act requires platforms to sustain a high standard of privacy, safety and security for children online. But many further improvements are needed to ensure children's personal data is handled lawfully, fairly, transparently, and only to the extent strictly necessary for providing services aligned with children's rights and best interests. These rights are effectively addressed in children's best interests through privacy-by-design and default combined with robust safeguards against misuse, commercial profiling and exploitation.

The Australian Online Privacy Code represents a unique opportunity to bring national regulation in line with international expectations and the lived realities of children online. As emphasised in General comment No. 25, this requires enforceable safeguards, not voluntary pledges by private companies. By combining legal safeguards with meaningful child consultation and technical design controls, the OIAC can realise children's rights in relation to the digital environment, fulfilling Australia's obligations under the UNCRC.

This post gives the views of the authors and not the position of the Media@LSE blog, nor of the London School of Economics and Political Science.

Featured image: Photo by SMA Fatemi on Unsplash

About the author

Kim Ringmar Sylwander

Dr Kim Ringmar Sylwander is a Postdoctoral Researcher at the Digital Futures for Children centre. Her research centres on how children and youth navigate technologically mediated environments, including issues related to sexual consent in online contexts, sexualised and racialised hate and young people's consumption of pornography.

Sonia Livingstone

Sonia Livingstone OBE is Professor of Social Psychology in the Department of Media and Communications at LSE. Taking a comparative, critical and contextual approach, her research examines how the changing conditions of mediation are reshaping everyday practices and possibilities for action. She has published twenty books on media audiences, media literacy and media regulation, with a particular focus on the opportunities and risks of digital media use in the everyday lives of children and young people.

Posted In: Children and the Media

THE LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE