Submission

Children's Online Privacy Code

July 2025

Submitted by

Katherine Berney

Executive Director

Working with Women Alliance

https://wwwa.org.au/

Acknowledgement of Country

The Working with Women Alliance (WwWA) acknowledge the Traditional Owners of the land on which we work and live. We pay our respects to Aboriginal and Torres Strait Islander Elders past, present and future. We value Aboriginal and Torres Strait Islander histories, cultures, and knowledge. We extend our respect to Aboriginal and Torres Strait Islander women who for thousands of years have preserved the culture and practices of their communities on country. This land was never surrendered, and we acknowledge that it always was and always will be Aboriginal land. We acknowledge the strength of Aboriginal and Torres Strait Islander people and communities. We acknowledge that Australian governments have been complicit in the entrenched disadvantage, intergenerational trauma and ongoing institutional racism faced by Aboriginal and Torres Strait Islander people. We recognise that Aboriginal and Torres Strait Islander people must lead the design and delivery of services that affect them for better life outcomes to be achieved.

About Us

The Working with Women Alliance (WwWA) represents two key portfolios: National Women's Safety (NWS) and National Women's Equality (NWE). The WwWA connects the critical areas of gender-based violence prevention and the advancement of women's economic equality and leadership, bridging these important policy fields for greater impact. We work with members and stakeholders, including the Australian Government, to provide expertise and advice on gender equality and women's safety.

Executive Summary

The Working with Women Alliance (WwWA) strongly supports the introduction of a robust and enforceable Children's Online Privacy Code. We emphasise that children's online privacy is fundamentally a safety issue, intimately linked to risks of digital abuse, grooming, and coercive control, particularly for girls who are disproportionately affected. While the current Privacy Act outlines obligations for entities to manage personal information responsibly, the proposed Code must explicitly address and mitigate foreseeable online safety risks to effectively protect children.

Key areas of concern include the growing role of artificial intelligence (AI) and automated decision-making in children's digital experiences. Recent investigations have revealed disturbing practices, such as AI systems being trained on children's images without consent, raising significant privacy and safety implications. The Code must explicitly regulate AI applications to safeguard children's rights, mandating transparency, consent mechanisms, and strict limitations on the use of children's data.

The Code's current approach to consent requires strengthening, particularly considering unsafe family contexts. Given the prevalence of technology-facilitated abuse within domestic violence situations, consent mechanisms must acknowledge power imbalances and coercion risks. Entities must implement age-appropriate, transparent pathways for children to understand, manage, and protect their personal information independently.

Further, while supporting the right to anonymity, the Alliance advocates for balanced measures that prevent misuse of anonymity for harassment. Entities should collect limited but necessary identifying information to hold users accountable for online behaviour while preserving their right to appear anonymously.

Additionally, Australia lacks a clearly articulated 'right to erasure.' The Alliance urges the adoption of this principle within the Code, empowering children with the right to delete personal data, especially sensitive or outdated information, aligning with international best practices.

The Alliance also calls for informed consent practices that meaningfully engage children, using diverse communication formats suitable for varied learning styles and cultural contexts. Moreover, default privacy settings should prioritise children's protection proactively, removing the expectation that young users bear the responsibility of opting out of potential privacy risks.

The Alliance's detailed recommendations aim to ensure that the Code robustly protects children's rights, dignity, and safety in the digital age.

Children's Online Privacy is a Safety Issue

To be most effective, the proposed Children's Online Privacy Code must acknowledge that privacy is a fundamental safety issue.

Online harassment often relies on the misuse of data, meaning that digital products and services that fail to safeguard children's personal information risk directly facilitating online abuse. Of the 96% of young people that use a social media platform, almost 1 in 10 have experienced image-based abuse.[i] Furthermore, nearly one in four children have experienced non-consensual tracking, monitoring, or harassment on an app or device.[ii] Girls, in particular, are disproportionately affected by online harassment and image-based abuse.[iii]

While the Privacy Act already places obligations on APP entities to manage personal information securely and fairly, the Code must clarify that these obligations extend to preventing foreseeable online safety risks.

<u>Recommendations</u>

- Strengthen the application of "best interest" to explicitly include safety from abuse, clarifying that protecting children from grooming, tech-facilitated abuse, and coercive control are central to best interest.
- Establish coordination between OAIC and eSafety Commissioner to reduce duplication and ensure privacy and safety are jointly addressed.
- Include within criteria used to determine whether an entity is within the scope of the Code the need for a risk assessment to assess how children's data could be misused and the level of impact.

Artificial Intelligence and Emerging Technologies

Despite the significant and growing role AI and automated decision-making is having in children's digital experiences, these systems are not adequately addressed in the proposed Children's Online Privacy Code, leaving a serious gap in supporting the online privacy of children.

Recent investigations have revealed that some of the world's largest AI models are trained using images of children, without the knowledge or consent of their families. Scraped from YouTube, school websites and online blogs, images of newborns, preschoolers, and young girls in swimsuits have appeared in public AI datasets, often with captions that include full

names and ages[iv]. These privacy violations, enabled and exasperated by AI, are specific, enduring, and deeply intrusive.

Critically, AI models are incapable of forgetting the data they are trained in and built on. Once a child's image or identifying details are used to train large language models (LLMs) or image generators, the data can be replicated and redistributed indefinitely, raising serious concerns about the handling of children's personal information.

Recommendations

- Explicit inclusion of AI systems and automated decision-making within the scope of the Code, recognising the growing role in profiling, targeting, content curation, and online interaction.
- Mandate that APP entities must disclose the use of AI systems.
- Require users to opt-in for AI systems to access information from social media accounts.
- Clarify that the use of children's data to train AI systems must be subject to strict limitations.
- Ensure that any APP entity developing or using AI systems is fully accountable under the Children's Online Privacy Code.

Consent and Unsafe Family Contexts

The proposed Children's Online Privacy Code places emphasis on consent as a safeguard for protecting children's privacy, particularly evident in APP 3 (collection) and APP 6 (use and disclosure). However, the Code currently lacks adequate guidance on how consent mechanisms should be understood and implemented in contexts where a child's home environment is unsafe.

For many children, the assumption that consent is given freely and voluntarily is not accurate. More than one quarter of domestic and family violence cases involve technology-facilitated abuse of children, most commonly monitoring and stalking. These types of instances are only increasing[v]. Children are deliberately given phones and having their social media accounts accessed by perpetrators with the intent to surveil and make unwanted contact[vi].

If the Code is to meaningfully uphold the best interests of the child, it must consider the conditions under which consent is sought and given. A purely procedural view of consent, without safeguards for power imbalances and coercion, does not serve children's safety.

Recommendations

- Clarify that APP entities should consider the potential for coercion or misuse in family contexts where personal information may be accessed or disclosed.
- Encourage services likely to be accessed by children to provide clear, age-appropriate pathways for children to understand and manage their own privacy settings, especially where they are old enough to provide direct consent under the Code.
- Ensure that notices and privacy information and training include examples of how data might be misused in family or shared device contexts.
- Implement disclosures for children to be aware of when parental control is enabled or when parental consent has been given and what data parents can view or access.

Anonymity and Personal Information

The Code requires entities to provide individuals with the opportunity to use a pseudonym or appear anonymously when engaging with the entity.

Users' right to engage anonymously is a positive protection of their personal information. However, NWS encourages the Code to consider how anonymity could be used in the context of online harassment and bullying.

Entities can only collect personal information that is 'reasonably necessary' to the functions or activities that take place on the platform. Collection must only be by lawful and fair means. Lawful and fair collection must require a high threshold for consent which stipulates what the data collection will be used for as a means of justifying that it is 'reasonably necessary.' This should include collection of information that can be used to identify anonymous users but is kept and protected by the entity.

Recommendations

- Entities should allow anonymous appearance where possible but always collect necessary information should the user abuse their anonymity.
- Collect personal information of all accounts so that users are still held responsible for their online behaviour and can be traced, but allow them to appear anonymously or without certain information – full name, birthday, address etc.
- Age assurance technologies should ask users to indicate their age rather than their birthday.

The Right to Erasure

Currently, there is no recognised 'right to be forgotten' in Australia. Under APP 11, APP entities are expected to delete personal data when "it is no longer needed." That means that children who have shared their personal information online, even if it was by mistake or without understanding what they were agreeing to, have no guaranteed way to delete it.

In contrast, the EU has had the right to erasure since 2018[vii]. Children and adults can ask for their personal data to be deleted when it's no longer necessary, when consent is withdrawn, or when it was collected unfairly. It's a basic right that the Albanese Government has already expressed support for[viii], along with 90% of Australians[ix].

The right to erasure is a concept that needs to be built into the Children's Online Privacy Code. The consultations that the OAIC did with children reported that they want the option to delete their data, especially once they turn 18 or stop using a service. They want control over their personal information, and they deserve it.

Recommendations:

- Amend APP 11 to include the right to erasure, providing an explicit timeline or expiry date on collected data.
- Amend APP 4 to remove the 'reasonably necessary' standard for the handling of unsolicited personal information, disallowing any collection of unsolicited personal information.
- Establish clear pathways for requesting the deletion of personal data, especially for sensitive information and inactive accounts.

Informed Consent

The way that online platforms currently get consent from children isn't working; clicking 'I agree' doesn't mean much to a child when reading terms and conditions that aren't appropriately written for them and when no other alternatives are offered. Consent should mean understanding what information is being shared, how it will be used, and what can be done if that decision changes.

There needs to be a shift towards engaging children in meaningful understanding of online privacy, starting with recognising that children don't all engage in the same way. Consent practices should reflect the way that children learn, whether that be through watching videos, listening to recordings, or reading. Privacy policies need to be available in different formats, and in multiple languages, so that children and their families can understand what they are agreeing to.

The consultations that the OAIC did with Reset Tech Australia further highlighted the need for more transparency in privacy codes. If information shared in the chat of an online game can be accessed by overseas entities or AI training datasets, that needs to be clear. Children want to know how their personal information is collected, used, and shared. Anything less should not be considered informed consent.

Recommendations

- Instruct entities to engage with stakeholders like Reset Tech Australia to develop children specific privacy policies and subsequent communication methods.
- Ensure notifications, terms and conditions, and educational videos that explain the privacy code are provided in multiple languages and formats, including audio and video to account for children with diverse needs and those from CALD backgrounds.
- Amend APP 6 to make secondary uses of personal information explicit, excluding any standard of reasonable expectation of secondary uses.

Default Settings

A significant gap in the Code is not requiring platforms to apply strong privacy default settings that limit data collection and sharing when a service is likely to be used by a child.

If a service is likely to be accessed by children, it should include default settings that protect their data, like turning off location tracking and data sharing with third party entities. The burden should not be on young users to opt out of risks they may not even recognise.

Recommendations

- Direct APP entities to enable default privacy settings for any children's account or platform likely to be accessed by children.
- Amend APP 7 to disallow entities to create 'reasonable expectations' that they may disclose personal information for the purposes of direct marketing, ensuring a completely opt-in option.

---

[i] eSafety Commissioner, 2025, *Digital use and risk: online platform engagement among children aged 10-15*, https://apo.org.au/sites/default/files/resource-files/2025-07/apo-nid331439.pdf

[ii] eSafety Commissioner, 2025, *Digital use and risk: online platform engagement among children aged 10-15*, https://apo.org.au/sites/default/files/resource-files/2025-07/apo-nid331439.pdf

[iii] eSafety Commissioner, 2019, *Online abuse disproportionately impacts girls and women — what parents need to know*, https://www.esafety.gov.au/newsroom/blogs/online-abuse-disproportionately-impacts-girls-and-women-what-parents-need-to-know#:~:text=We%20have%20received%20over%20980,of%20these%20victims%20are%20female.

[iv] Ange Lavoipierre, 2024, *The world's biggest AI models were trained using images of Australian kids, and their families had no idea*, ABC News, https://www.abc.net.au/news/2024-07-03/ai-generated-images-privacy-children-human-rights/104043414

[v] eSafety Commissioner, 2024, *Supporting children experiencing family and domestic violence*, https://www.esafety.gov.au/key-topics/domestic-family-violence/support-service-resources/supporting-kids-dealing-with-tech-abuse

[vi] Wesnet, 2020, *Second national survey on technology abuse and domestic violence in Australia*, https://wesnet.org.au/wp-content/uploads/sites/3/2020/11/Wesnet-2020-2nd-National-Survey-Report-72pp-A4-FINAL.pdf

[vii] Art. 17 GDPR – Right to erasure ('right to be forgotten') - General Data Protection Regulation (GDPR)

[viii] Australian Government, 2023, *Government Response Privacy Act Review Report*, https://www.ag.gov.au/sites/default/files/2023-09/government-response-privacy-act-review-report.PDF

[ix] Office of the Australian Information Commissioner, 2023, *Australian Community Attitudes to Privacy Survey 2023*, https://www.oaic.gov.au/engage-with-us/research-and-training-resources/research/australian-community-attitudes-to-privacy-survey/australian-community-attitudes-to-privacy-survey-2023