PO Box 621,
Collins Street West,
VIC, 8007

P: +61 3 9607 7101
M: office@cprc.org.au
www.cprc.org.au

CPRC
Fairer markets for Australians

Submission to OAIC: Consultation on OAIC Children's Online Privacy Code

31 July 2025

Commissioner Carly Kind
Privacy Commissioner | Office of the Australian Information Commissioner

Submission made via: **copc@oaic.gov.au**

Thank you for the opportunity to provide feedback on the Issues paper for the OAIC Children's Online Privacy Code (the Code).

Consumer Policy Research Centre (CPRC) is an independent, not-for-profit, consumer think-tank. CPRC aims to create fairer, safer and inclusive markets by undertaking research and working with leading regulators, policymakers, businesses, academics and community advocates. Below is our submission on specific aspects of the Code along with broader reforms we wish to highlight, in recognition that this Code is not in isolation of the Privacy Act which is well-overdue for reform.

Question 4.5 Do you have any specific views on how APP 1 should be applied or complied with in relation to the privacy of children?

CPRC recommends that the scope of personal information that will be captured within the Code be broader than the definition that is currently within the Privacy Act. The Code should apply to a child's data that could be reasonably identifiable which includes being capable of being distinguished from all others even if the exact identity is not known.[1] For example, the scope should cover data such as geo-tracking, online identifiers, physical, physiological, genetic and even behavioural predictions or preferences. We believe this requirement would not be contrary nor inconsistent with the Australian Privacy Principles (APPs) but would be an additional requirement, which as noted in the Issues Paper Executive Summary would not out be out of scope for the Code. It would help elevate the expectations towards the protection of children's privacy online, which ideally in future, should apply to all Australians.

Question 9.1 How can APP entities obtain genuine consent from children, or their parents or guardians, for the use or disclosure of their personal information, while ensuring that they comprehend the implications of such use or disclosure?

CPRC recommends that the Code include an explicit requirement that obtaining consent of any form does not include the use of deceptive and manipulative practices, also known as 'dark patterns'. Dark patterns are design features that are built into websites and apps that aim to steer people's choices, often not in their best interest.[2] CPRC's research has found that 83% of adult Australians have been negatively impacted through the use of dark patterns. It can cost people their time, money, control over their privacy and ultimately impact their wellbeing. For example, our 2022 study revealed that dark patterns can significantly impact people's control over their privacy with

[1] In 2023, CPRC along with other consumer groups supported the definition of personal information recommended via Salinger Privacy's submission on the Privacy Act Report: https://www.salingerprivacy.com.au/wp-content/uploads/2023/03/23-03-31_Privacy-Act-Review_Salinger-Privacy-Submission.pdf.
[2] CPRC, 2022, *Duped by Design – Manipulative online design: Dark patterns in Australia*, https://cprc.org.au/report/duped-by-design-manipulative-online-design-dark-patterns-in-australia.

one in four adult Australians (25%) sharing more personal information than they wanted.[3] We expect results would be similar to or even higher for children faced with dark patterns but note this is a research gap which deserves further funding to explore.

CPRC's 2025 research into unfair digital gaming practices found that more than half (52%) of adult digital game players encountered some form of privacy harm in the past 12 months including accidentally signing up to something, creating an unwanted account online and sharing more personal information than they intended. [3] This is particularly pertinent considering that many of the digital games we identified in our research target children.

In addition to the above requirement, CPRC recommends that when a person has refused to consent, an APP entity should not continue to request or nag the person and should instead ensure that an alternative, less personalised version of the service is still available for the person to use. This model currently exists within the EU Digital Markets Act (DMA) and, if implemented within the Code, could provide a more robust protection to children's online experience and use of their data.[4]

Article 5-2 of the DMA includes an obligation to not nag an individual for a minimum of one year if they have refused consent for their data to be collected or used by the entity. The DMA also has an obligation, for businesses to which the DMA applies to, to ensure that those individuals who have not consented to their data being collected or used but would still like to use the service, the alternative, less personalised service should, "*...not be different or of degraded quality compared to the service provided to the end users who provide consent, unless a degradation of quality is a direct consequence of the gatekeeper not being able to process such personal data or signing in end users to a service.*" When it comes to withdrawing consent, the obligation clearly states that it should not be more difficult to withdraw consent than to provide it in the first place.[5]

Question 10.1 Can an APP entity ensure that it creates a 'reasonable expectation' that it may use of disclose children's personal information for the purposes of direct marketing? And if so, how?

Question 10.3 Do you have specific views on how APP7 should be applied or complied with in relation to the privacy of children?

CPRC recommends that APP entities under the Code should be prohibited in partaking in any aspect of targeted advertising towards children from collection and sharing of data to use of data to directly market to children. In June, a roundtable led by Reset.Tech Australia, bringing together over 20 experts from academia and civil society, confirmed that targeted advertising as a violation of children's rights due to the data handling that is required to implement it.[6] Experts also noted that obligations within data protection laws across many jurisdictions overseas including the UK, Ireland and the EU make it clear that children should not be profiled.

CPRC's consumer research confirms that Australian adults have a clear discomfort with personal information being used for targeted advertising. Less than 10% of Australians are comfortable with how targeted advertising is currently approached in Australia, which is opt-in by default and complex or without clear pathways to opt-out. Close to half are not comfortable with companies targeting them based on their online behaviour (46%) or their personal characteristics (49%).[7] Joint

---

[3] *Ibid.*
[4] Gupta, C., 2025, *Made to Manipulate: The impact of deceptive online design practices on wellbeing and strategies to mitigate harm*, https://cprc.org.au/report/made-to-manipulate-report.
[5] Gupta, C., 2025, *Made to Manipulate: The impact of deceptive online design practices on wellbeing and strategies to mitigate harm*, https://cprc.org.au/report/made-to-manipulate-report.
[6] Reset.Tech Australia, 2025, Targeted advertising & the Children's Online Privacy Code, https://au.reset.tech/news/targeted-advertising-the-children-s-online-privacy-code/.
[7] CPRC, 2023, *Not a Fair Trade – Consumer Views on how businesses use their data*, https://cprc.org.au/report/not-a-fair-trade-consumer-views-on-how-businesses-use-their-data/.

CPRC and UNSW research has also found that 71% of Australians feel they possess little to no control over businesses sharing their personal information with other entities.[8]

Some in industry will bemoan restrictions on targeted advertising online for children. We note that contextual advertising online will still be allowed and very appropriate. For example, a company with an educational product for children will still be able to advertise on websites that are made for children (or their parents as the likely purchasers of a product). A ban on targeted advertising to children is not a ban on advertising, only the extensive tracking and tracing of children's online activity currently used to fuel advertising online.

Given that such a high percentage of Australians are uncomfortable with mechanisms of processing data that surround targeted advertising, it is clear that direct marketing should not factor as part of a child's online experience.

Broader reforms to ensure effectiveness of the Code

While the Code is a critical step forward in ensuring stronger privacy protections for Australian children online, its effectiveness will significantly depend on how APP entities are held accountable in implementing the Code and what support is available for children and their parents or guardians if things go wrong.

CPRC recommends that as part of developing the Code, the OAIC urges the Federal Government to strengthen its powers as a regulator so it can effectively stop harmful behaviour and practices before widespread harm occurs. To create an effective ecosystem for children's online privacy protections, the Government must ensure the regulator is adequately resourced with the capacity and capability to monitor and enforce privacy breaches in this complex environment.

Positive obligation on APP entities

CPRC recommends there be a positive obligation on APP entities captured under the Code to have their systems independently audited periodically and to submit upfront to the regulator how it meets the requirements under the Code. This will ensure that information on compliance is coming to the regulator instead of the regulator continuously seeking it out or the burden being placed on individuals or civil society to identify and report harm. Elements of this model currently exist in the EU Digital Services Act which requires designated entities to proactively assess risks and provide relevant data to authorities to assist in understanding the impact of the platform on its users and to help mitigate issues early.[9]

Currently regulators largely rely on reports from individuals or civil society, identifying harm after it takes place. The majority of the onus cannot continue to remain on consumers and consumer groups to identify and report breaches. This is not sustainable in a digital environment where there are complexities in understanding how consumer data is collected, used, and passed on to other businesses. Instead, regulators need to proactively uncover harm that is currently obfuscated. Regulators should be pushing businesses to be radically more transparent about how they use consumer data.

Enforcement

CPRC recommends that the OAIC and the Federal Government consider broader enforcement strategies beyond pecuniary penalties to ensure APP entities are held accountable for complying with the Code. This could include obligations such as data disgorgement. This is where an entity in

[8] Kemp, K., Gupta, C., Campbell, M., 2024, *Singled Out - Consumer understanding — and misunderstanding — of data broking, data privacy, and what it means for them*, https://cprc.org.au/report/singled-out.
[9] Gupta, C., 2025, *Made to Manipulate: The impact of deceptive online design practices on wellbeing and strategies to mitigate harm*, https://cprc.org.au/report/made-to-manipulate-report.

breach of the Code would be forced to delete or surrender data, algorithms and even products that it has designed based on what it gained through illegal practices.[10]

Given that the Code will apply to some very large businesses, such an enforcement strategy would ensure that breaching the Code is not seen as 'just the cost of doing business'. For such businesses pecuniary penalties will not be enough to dissuade non-compliant behaviour. For example, it was reported in 2022 that Meta had put aside EUR 3 billion in its forecasted budget to simply cover payment of GDPR fines.[11] Penalties shouldn't be a budget line item but a meaningful deterrent.

Redress

CPRC recommends that APP entities be obligated to have clear internal dispute resolution (IDR) processes and that the OAIC and the Federal Government consider developing a clear and accessible pathway for redress.

CPRC's consumer research confirms that adult Australians are not confident in finding or accessing support mechanisms for when things go wrong online:

- 50% do not know where to seek help if they have a problem with how a company collects, shares or uses their personal information.
- 46% do not know where to seek help if their data is hacked.
- 46% do not know who to seek help from if they believe their personal information is being used in a way that's causing them harm.
- Only 18% are confident that they will be compensated if they've been left worse-off because of how a company collected, shared or used their information.[12]

CPRC believes that in addition of placing clear IDR expectations on APP entities, there is merit in a more holistic approach to external dispute resolution, such as via the establishment of a Digital Ombudsman that can provide support on all facets of a digital experience, including privacy.

There must be effective dispute resolution pathways to enable Australians to seek redress for when things go wrong in the online space. As Australians, including children, increase their engagement online, a Digital Ombudsman needs to be adequately resourced to meet benchmarks for industry-based customer dispute resolution to ensure Australians can effectively resolve any disagreements that will arise.

CPRC welcomes the opportunity to discuss any aspects of this submission further. If you have any questions, please contact Chandni Gupta via email chandni.gupta@cprc.org.au.

Yours sincerely

[redacted]

[redacted]

[10] *Ibid.*
[11] Gupta, C., 2025, *Made to Manipulate: The impact of deceptive online design practices on wellbeing and strategies to mitigate harm*, https://cprc.org.au/report/made-to-manipulate-report.
[12] CPRC, 2023, *Not a Fair Trade – Consumer Views on how businesses use their data*, https://cprc.org.au/report/not-a-fair-trade-consumer-views-on-how-businesses-use-their-data/.