
Submission to OAIC: Exposure Draft of the Children's Online Privacy Code

5 June 2026

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 Exposure Draft and Explanatory Statement for the OAIC Children's Online Privacy Code (the Code).

The Consumer Policy Research Centre (CPRC) exists to create fairer markets. We do this by researching and championing reforms to make consumers' lives better. We focus on areas where people need the most support in improving and using their rights, including housing, sustainability and online markets.

Broadly CPRC is supportive of the introduction of the Code. Below are our recommendations on specific aspects of the draft Code that we believe would help strengthen the Code further:

Recommendation 1: Amend Section 14(3)a to mirror wording in the Unfair Trading Prohibition Bill relating to manipulation and deception

CPRC supports the inclusion of prohibiting consent through manipulative, deceptive and misleading practices as noted in Section 14(3) of the draft Code. However, there is an opportunity to clarify this provision by strengthening further the concept of manipulative and deceptive practices within the Code. For example, the current Unfair Trading Prohibition Bill specifically outlines manipulative and deceptive practices as:

"...creating an environment (including by using design elements in digital interfaces) which places the consumer under unreasonable pressure in relation to, or obstructs the consumer from, making or fulfilling the consumer's decision."¹

This helps capture more clearly the concept and use of dark patterns, which are prevalent across any online experience within Australia. 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 one in four adult Australians (25%) sharing more personal information than they wanted. We expect results would be similar 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

¹ See Part 2-4 Unfair trading practices Section 28B(6c):
https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;db=LEGISLATION;id=legislation%2Fbills%2Fr7468_first-reps%2F0001;query=Id%3A%22legislation%2Fbills%2Fr7468_first-reps%2F0000%22;rec=0.

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.

Recommendation 2: Amend Section 14(3) to include an additional provision for a child to not be nagged if consent is refused

CPRC supports the inclusion of Section 14(3)c which confirms that access to service should not be denied if consent is refused unless strictly necessary for the purposes of the service. This provision should be made stronger by stating that when a child has refused consent, an APP entity should not continue to request or nag the child to provide that consent. 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.² 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.

Recommendation 3: Amend Section 29 to ensure children are not opted-in by default to direct marketing

OAIC should amend Section 29 by making opting out of direct marketing easier, it should instead include provisions that ensure that children are not opted-in to direct marketing in the first place. There should also be provisions included that dark patterns are not utilised to encourage children who have opted out to re opt-in to direct marketing.

At a minimum, Section 29 should include an additional provision that states when a child has opted out of direct marketing, an APP entity should not continue to request or nag the child to re opt-in to direct marketing. This should cover practices including the use of dark patterns such as Confirmshaming, False Hierarchy and Nagging.³

Recommendation 4: Add case study examples and cite Australian research in the Explanatory Statement

The OAIC should add case studies and cite practical research throughout the Explanatory Memorandum to help bring the Code to life. This will also support businesses to understand their obligations in a more meaningful way. As an example, the current Explanatory Memorandum for the Unfair Trading Prohibition Bill contains detailed examples of practices such as designing the cancellation process of a gym membership as part of the subscription provisions within the Bill (Paragraph 1.102).⁴

The Explanatory Memorandum for Unfair Trading Practices Bill also includes detailed research findings, such as citations from Australian and international research. It helps to provide context for businesses when implementing their own practices. For example, the current Explanatory Memorandum for the Unfair Trading Prohibition Bill outlines information on different forms of dark patterns, and cites research from various sources including the Consumer Policy Research Centre so those adhering to the provisions can have a more holistic view of the obligations.

At a minimum, we recommend that the OAIC includes a clear definition of dark patterns in the Explanatory Memorandum as design features that are built into online interfaces that aim to steer people's choices which are not in their best interest and include examples of key types of dark patterns noting how these could breach Section 14(3). We also recommend that the OAIC update the

² 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>.

³ CPRC, 2022, *Duped by Design – Manipulative online design: Dark patterns in Australia*, <https://cprc.org.au/report/duped-by-design>.

⁴ See *Competition and Consumer Amendment (unfair Trading Practices) Bill 2026 Explanatory Memorandum*: https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22legislation%2Fems%2F7468_ems_f67a492e-01ee-4b22-b61e-bfa097d98194%22.

Explanatory Memorandum to incorporate key research through citations to help complement the definitions and case study examples. In terms of dark patterns, we recommend that the OAIC cite the following research from Consumer Policy Research Centre:

- *Duped by Design*, which was Australia's first-ever research into the impact of dark patterns on Australian consumers: <https://cprc.org.au/report/duped-by-design>
- *Playing the Player – Unfair digital gaming practices and their impact on Australians*, which revealed that over half of Australian players encountered privacy harms due to dark patterns: <https://cprc.org.au/report/playing-the-player/>.

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.

As part of introducing the Code, the OAIC should urge 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.

Enforcement

The OAIC and the Federal Government should 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 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.⁵

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.⁶ Penalties shouldn't be a budget line item but a meaningful deterrent.

Redress

APP entities should 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.

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 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>.

- 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.⁷

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 me via email: chandni.gupta@cprc.org.au.

Yours sincerely



Deputy Chief Executive Officer and Digital Policy Director

Consumer Policy Research Centre

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/>.