Submission to the Online Privacy Bill Exposure Draft

Child Wise is pleased to respond to the Australian Government's invitation to make a submission to the Online Privacy Bill Exposure Draft.

The distinction between the online and the non-digital world is becoming more obscure every day, particularly in the lives of children and young people.

The rights of children and young people online are as important as those in the non-digital world.

There is significant potential for the Online Privacy Bill to lift the bar, and to advance children's rights in the digital world.

While this is a submission from Child Wise only, we have collaborated with many others to inform our perspective, particularly, Reset Australia, The Australian Council on Children and the Media and, the Alannah & Madeline Foundation. We are grateful for their expertise and willingness to work with us on this critical issue.

Our submission is structured in two sections: key strengths & observations, and, areas that require further consideration.

Key Strengths & Observations

1. **We support the requirement that platforms must consider children's best interests in their data processing**

    - This must be the 'central' approach in privacy protection, and data processing, for children.

    - The Code would need to outline very clearly what 'best interests' means in practice, and Code Developers must be given a clear set of essential requirements. We support definitions of the United Nations Convention of the Rights of Child.

    - The Code must outline that children's best interests should be considered in:

        - Recommender systems and algorithms for children, which train on and process their data
        - Automated decision making and profiling, where it processes children's data

- Digital marketing and commercial profiling, such as surveillance advertising which processes their data
- Testing for 'persuasive' design, where children's data is processed in A/B tests for instance

2. **We support the requirement that platforms must take reasonable steps to verify the age of their user.**

- The current system allows children to join in a completely 'friction free' process. While no (current) mechanism to assure age is perfect, adopting one or more reasonable steps may add some friction into the system to discourage very young users from joining age-inappropriate platforms.

- However, the Code would need to make these reasonable steps for age assurance inclusive, to ensure that children and young people's access is not reduced nor affected by socio-economic factors. For example, requirements for identification documents such as passports or birth certificates will have a disproportionate negative impact on some young people.

- Any age assurance moves must be privacy preserving. Young people should not have to hand over more data to ensure their data is treated age-appropriately.

- The requirement for online platforms to assure the age of their users may also increase the ability of platforms to better police their minimum age requirements, which is also welcome.

- Finally, while we welcome this focus, this requirement is unlikely to 'move the dial' much in terms of advancing children's rights in the digital world. Platforms already have adequate knowledge to effectively assure the age of their users, and yet at times, continue to provide high risk, exploitative platforms to children. While moves that may enable the prevention of those under 13 from accessing services are welcome, they will not improve the situation for users aged 13 plus.

- We also note that the minimum age requirement of 13 does not reflect any research around what age these platforms might cause less harm, and in that sense, it is an arbitrary cut-off that does not seem to be evidence-based.

3. **We note the proposed requirement that platforms must obtain consent from parents or carers to process the data of under 16-year-olds and take reasonable steps to verify parents or carers. We understand the intent of this requirement but note the possibility that this may disadvantage marginalised young people.**

- It is a welcome requirement for platforms to move towards basic, reasonable steps to seek parental consent, even if such moves currently are technically difficult and imperfect.

- We note that under the current system, most major online platforms neither seek nor obtain any parental consent at all for data processing for children, despite Australian guidance stipulating that consent should be obtained for under 15-year-olds.

- The Code however would need to outline that the reasonable steps for verifying parental identity must not disadvantage marginalised young people, to ensure equitable access. That is, this measure should not prevent young people from accessing digital services because their parents or carers don't have access to email or technology.

Areas that require further consideration

1. **Children's and young people's right to participate must be respected and clearly articulated.**

    - Significant aspects of the Bill aim to protect children and young people.

    - Children and young people will be significantly impacted by this Bill.

    - As such, we would like to see requirements for children and young people under 18 years to be consulted in:

        - The development of the Code
        - Any reviews of the Code and
        - The ongoing operation of the Code

2. **The Bill should cover a broader scope of industries**

    - The Bill needs to be expanded to ensure all services used extensively by Australian children are covered. Currently, EdTech providers, most games and commercial health apps (who collect sensitive data) wouldn't be covered.

    - To ensure that the full range of digital services and platforms children use falls into scope, the definition of 'large online platform' needs to change.

        - The current definition of large platforms is 2.5million end-users (or 10% of the population).
        - At June 2019, Australia had just over 5.6m residents aged below 18.
        - Almost half Australian children could use a platform targeting children that was not covered by the code, and it would take over 45% of Australian children to use a service before it was covered by the Code.

3. The Bill must specify that the Online Privacy Code must align with, and build on, the Codes and Expectation of the Online Safety Act

- The Online Privacy Bill should acknowledge the Online Safety Act, the Codes and the Basic Online Safety Expectations being developed under it, and outline that it is intended to further enhance children's online experiences.

- There is a risk that the development of two industry codes in parallel, one targeted at privacy and one at online safety, will be seen as confusing and create gaps for compliance and enforcement monitoring.

- This fragmentation is further enhanced by the Basic Online Safety Expectations, and the fact that the Codes are overseen by different Commissioners with related, yet different priorities.

4. The expectation that the Code must be promoted once developed, should be included in the Bill

Children, young people and families should know about these new protections, so they can better exercise and protect their rights.

There should be requirements around promoting the Code when it is released to ensure it can be meaningfully used by families and young people.

By ensuring the Code is promoted, it will help empower children, young people and their parents/carers to understand their rights.

We thank you for the opportunity to contribute to this critical issue.

Kind regards

Natalie Siegel-Brown
Managing Director
2 December 2021