

To: Office of the Australian Information Commissioner

Draft Children's Online Privacy Code (consultation for industry, civil society, academia) ('the Code')

Dear Committee,

I Introduction

This submission is authored by [REDACTED] and I am a legal academic with areas of expertise within the fundamental rights domain. My most recent research focused on the privacy impacts of the 'social media ban' in Australia and highlighted my concerns regarding the potential mismanagement of sensitive information of Australian residents who would be compelled to verify their age via age assurance technology.¹ This submission will discuss the implications of the laws proposed under the Code and outline the potential impacts that may result from its implementation in its current form.

Of course, this submission will include a higher focus on the elements to which I believe can be improved or should be reconsidered – as is the nature of submissions. However, this is not to take away from the beneficial impact that this Code could have with regard to safeguarding children's online privacy and informing them of the information that they must consent to sharing to use a service provided on the internet.

II Commentary on the Code

1. Section 13 reveals that the age of consent is 15 years of age or older, with children under this age requiring consent from a "person with parental responsibility for the child". This raises an issue surrounding the enforcement of other similar legislation, like the 'social media ban' that is enforced via the *Online Safety Act 2021* (Cth). As this Code and the social media ban have two different ages, 16 and 15 respectively, there may be an unnecessary burden placed on age-restricted social media providers who are also captured within the parameters of the Code – as they will now have two separate compliance pathways and consent barriers that encapsulate two different ages

¹ Hatzikalimnios, A. (2026). Privacy in the age of data breaches – the 'social media ban' in Australia. *Journal of Media Law*, 1–34. <https://doi.org/10.1080/17577632.2026.2659376>.

of Australian children. The Australian Privacy Principles restrict the ability to use previously collected data for purposes not disclosed within the original consent barrier, so there remains an increased burden in managing two different ages for eerily similar legislative amendments that are primarily focused on protecting Australian children from internet harm. A plausible solution could be creating another consent barrier, in which a whole separate pipeline of document management processes for age assurance may arise.

Recommendation 1: Consider shifting the age under this Code from 15 to 16 to be in-line with other similar legislation to reduce the exchange of sensitive information required for Australian children to use the internet.

2. Section 7 deals with the application of the Code on relevant platforms that include social media services, electronic services or a designated internet service. Subsection ‘b’ outlines activities that are “primarily concerned” with children, which can often be easily ascertained via the purpose of an application – for example, the ‘YouTube Kids’ offering from YouTube. At face value, this should not be too difficult to determine objectively for platforms. However, the language “likely to be accessed by children” seen under subsection ‘a’ is a little more ambiguous and may cause greater difficulty in its application by service providers bound by the Code. A concern is, who determines whether a service is likely to be accessed by children? Is it an external process that is to be administered by the OAIC or is it an internal compliance issue to be administered by service providers bound by the Code? In either case, there seems to be an initial, burdensome undertaking to be completed by individuals who are tasked with making these determinations and the continued monitoring of service expansion. This is just something to consider.
3. Section 8(1) outlines that entities must take “steps that are reasonable” to determine the age of the user. The Code’s explanatory statement outlines that entities will implement “age assurance”, which can encompass age inference, estimation or even age verification. Data within the information economy is more valuable than ever and including further methods of age verification will, inevitably, result in the greater amount of sensitive information being held by entities that can be accessed by bad actors if the information were to be mishandled or mismanaged. Of course, mistakes can happen – but dealing with the sensitive information of Australian children should take the highest priority of protection and entities should prioritise the limitation of such data that is processed.

Recommendation 2: Encourage entities to implement new consent barriers to use previously, consensually, collected information to determine the age of end-users

and prioritise age inference. Language could be inserted into Section 8(1) to clearly outline this, as the current language is ambiguous and may lead to companies utilising stronger methods to collect information at first instance.

4. Section 10 frequently refers to the phraseology “best interests of the child” throughout but it does not discuss any of the important preamble included within the Code’s explanatory statement that outlines the underpinnings of children’s rights. If a company were to use similar age assurance technologies relied upon to enforce the social media ban, like the facial scanning technology, there is the possibility that a data breach could result in the exposure of biometric data that will allow bad actors to create unlawful or explicit content from such material. A recent example of this occurred in the United Kingdom where a school shared a photo of their students on one of its social media pages. The photos were then downloaded by bad actors, inserted into Generative AI tools, turned into child sexual abuse material, and were accompanied by threats stating that the photos would be published if the school did not pay the blackmailer’s money to prevent their publication.² In Australia Generative AI technology has been used to produce ‘intimate images’ that were generated and shared without the consent of the individuals presented in the deepfake material.³ These technologies are only growing more sophisticated in their abilities and it is imperative that the protection of sensitive data, especially biometric data, of Australian children be at the forefront of policy decisions within the Code and its adoption by entities.

Recommendation 3: Include language from the explanatory statement to emphasise the risks associated with the mishandling or over-collection of sensitive information of children and the impacts this could have on broader society.

5. Section’s 15 through 19 include essential protections with regard to the way Australian children look to engage with service providers bound by the Code. There is, however, one issue with Section 15(4)(b), which necessitates that any data collected for age assurance by entities under the Code must not be held for longer than 12 months. In-line with the sentiments held in paragraph four (4) of this submission, this retention period seems excessive and not aligned with Section 8(4) of the Code. In addition, Section 15(4) refers to the language used in paragraph 3(b) of

² ‘UK schools should remove pupils’ online photos as AI blackmail threat grows, say experts’ (*The Guardian*) <<https://www.theguardian.com/technology/2026/may/08/uk-schools-remove-pupils-photos-online-ai-blackmail-threat-grows>> accessed 25 May 2026.

³ *eSafety Commissioner v Rotondo (No 4)* [2025] FCA 1191.

Section 15, to which I believe should actually reflect reference to paragraph 3(c), as this includes the word “period” referred to in 15(4)(b).

Recommendation 4: Reduce the period in which entities can rely on consent to handle sensitive information from 12 months 1 month. This would encourage entities to swiftly process and destroy any information it obtains, as well as reduce the amount of information that may stay in ‘limbo’ whilst administering compliance with the Code.

6. Finally, I commend the construction of Division 6, as it appears to place an emphasis on empowering children to understand how their information is being controlled and/or monitored by those with parental responsibility. In addition, this component, if implemented well by entities, could have a positive impact on the way children interact with online platforms and encourage them to understand the risk such services can pose to their privacy if they are not careful when using them.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]