[redacted]

[redacted]

[redacted]

[redacted]

Responses to the questions below are in [redacted] private capacity and do not represent any organisation she may be affiliated with. [redacted] considers her specialisation in privacy law and children. [redacted] is not a 'tech wizard'.

[redacted]

Specific questions are answered below which are tailored to [redacted] expertise. Responses are guided through the lens as a privacy law scholar, and not as a technology specialist. General comments are added at the end.

Question 1

1.1 Are there additional APP entities, or a class of entities, that should be covered by the Code? Please provide reasons or evidence to support your view.

Educational technology ('edtech') providers must be caught by the code. The problem is if they operate outside of the code there risks a lacuna of enforcement between state privacy legislation, where edtech is for the provision of educational services, and those APP entities operating on a commercial scale such that they would otherwise be caught by the scope of federal privacy law. There needs to be a way to protect the information of a child in an educational technology setting. Moreover, the Reset Tech research highlighted there needs to be greater consideration with respect to consent to using a particular educational technology.

Question 2

2.1 What threshold should determine when a service is considered 'likely to be accessed by children'?

'Likely to be accessed by children' is in many respects an ambiguous term. Children are unlikely to access breast screening or bowel cancer websites aimed at those in middle to later age, however, they might still access websites or services provided by a health system. Furthermore, websites not considered likely to be accessed by children could also contain information relevant to a child.

Traditional websites tend to be built according to the information the provider considers relevant. Therefore, as an example a website for a sporting association, would likely to be accessed by children searching for ways in which to join the a club relevant nearby. However, an individual club in the sporting association might not necessarily consider that the site would fall within the scope of 'likely to be accessed by children'. The definitions raises unintended consequences and risks infringing on the right to accessing information. Furthermore, many sporting or music clubs use a social media platform for more immediate forms of communication, which might not be available for young people.

2.2 'Likely to be accessed by children' is the same standard as the Age Appropriate Design Code. Is there any evidence as to the practical effectiveness of the threshold in that context?

Likely to be accessed by children is considered ambiguous. For example, children carrying out research for a school project about the history of a particular topic, or a problem they have been tasked with at school, are then going to access services which were not necessarily considered 'likely to be accessed by children'. Therefore, the Age Appropriate Design Code should be considered alongside the school curricula created by state and territory governments.

2.4 What role, if any, should age gating or other access control mechanisms play in meeting obligations under the Code?

2.5 Are there alternative approaches APP entities could take to meet their obligations under the Code, beyond age gating or age verification methods? If so, is there any evidence on the impact of such approaches on children's access to services or privacy outcomes?

I consider the answer to both these questions through the lacuna of human rights in Australia. Professor Sarah Joseph alluded to the risks from the Online Social Media Minimum Age legislation in her piece 'Banning under-16s from social media may be unconstitutional – and ripe for High Court challenge'.

Age verification methods risk invading the privacy of young people in a way which compromises their access to information. A careful balance is required.

Question 3

3.1 Would age-based guidance be appropriate and assist APP entities in tailoring protections and interfaces appropriately and effectively?

Age-based guidance could support APP entities; however, it could again be helpful to link with educational curricula to understand child learning profiles. As noted in the Reset Tech research, many children felt they had to consent to a particular technology and their privacy policy because they felt compelled to use a product mandated by school.

3.2 In terms of providing guidance for the processing of children's personal information by APP entities covered by the Code, how appropriate do you consider the above age ranges would be?

The age-based guidance could provide some support to APP entities, however, on the basis of the feedback from the Reset Tech research, children should be considered a special category under the age of 18 and until they have finished

schooling. The 'high privacy' approach adopted in the UK could be considered in Australia.

Question 4

4.3 What should be considered under the 'reasonable steps' test when implementing internal practices, procedures and systems for managing children's personal information?

A de minimis principle should be adopted in respect of taking 'reasonable steps' for managing children's personal information. This could mean that as little information is taken as possible for the shortest amount of time. For example, for an edtech provider this could mean that only the name of the child, school and school year of the child is taken. This enables appropriate information to be loaded according to the school age and learning needs.

General Comments

Australia needs to consider the Age Appropriate Design Code through the lens of a relatively small jurisdiction. In order to fulfil its obligations under the United Nations Convention on the Rights of the Child children's privacy needs to not only be protected, but children need to be supported to access information in a way that those living in a generation of 'hard copy' and 'physical libraries' did not consider at the time of drafting the UNCRC.

The United Kingdom has adopted an 'Age appropriate design: a code of practice for online services' which has adopted a 'high privacy' by default setting for children. This is particularly relevant in respect of APP 2 to support children accessing online services in an anonymous or pseudonymous manner. By adopting a 'high privacy' system by design, this supports children's privacy and right to access information as a default mechanism.

Question 3 considered age appropriate guidance, and specifically the appropriate way in which to communicate privacy terms and conditions with children. Recent research has considered the use of emojis in legal contracts. This could suggest that if a privacy policy is 'distilled', suitable for a child or young person into, for example, pictures or emojis, that pictures and emojis can lead to different outcomes, dependant on the reader.

One of the key elements of my PhD was the ability to leave one's past behind. This is particularly relevant to young people and children wishing to correct or erase information (APPs 10, 12 and 13). If adopting both a privacy by design and a 'high privacy' approach this should consider first and foremost the biological development

of children. Some of the Reset Tech research has shown that the young people consulted would like better control over their information. Nonetheless, the Reset Tech research does not consider those under 13 years of age. I await the outcome of the earlier consultation with parents and guardians to provide guidance in this area. Nevertheless, prior to secondary education, there should not be a commercial trail of children's information. The former Attorney General stated at the second reading of the Privacy and Other Legislation Amendment Bill 2024 "[I]t's been estimated that by the time a child turns 13, around 72 million pieces of data will be collected about them." Commonwealth, Parliamentary Debates, House of Representatives, 12 Sept 2024, 6651 (Mark Dreyfus, Attorney General).

This volume of information cannot continue to be collected from and about children. I look forward to further consultation prior to the adoption of an age appropriate design code.

[redacted]