

Phase 2 Industry Codes Response

Submission

I am submitting this submission as an individual. I am a member of the Esafety youth council; however, my submission is not representative of eSafety or the eSafety youth council as a joint submission is not being coordinated.

Age assurance

The user base of many social media and online platforms are predominantly young people, many of which are under the age of 18. While the age assurance trial continues in Australia, I find it unwise to draft codes related to age assurance before there are more concrete regulations and directions around age assurance. The debate around age assurance involves matters of privacy, and I find that public views on age assurance mainly involve fear of data theft and privacy infringements as the most reliable forms of age assurance would involve providing sensitive documentation (such as passports, birth certificates, forms of ID) which many people will not be eager to provide to large digital platforms. Biometric forms of age assurance are notoriously unreliable, for example voice or face scanning. As a young person in Australia, many younger social media users who happen to look older than they are, can easily bypass biometric age assurance measures. On the other hand, there are many younger social media users (whether they are below or above the age of 18) who are not eager to provide images or voice recordings to large social media platforms.

However, extending the use of digital 'ecosystems' as described by eSafety and within the draft codes, currently seems the most reasonable direction as digital 'ecosystems' are already a growing tool. Similarly, connected accounts between younger users and their guardians (parents or carers), such as the Messenger Kids function on Facebook can also provide a reliable supervision connection between carers and young children so that the focus is on carer-discretion rather than in-app or in-platform based restrictions and filtering (even though they are independently successful to an extent).

Online Safety Measures

Building upon young children's exclusive social media or digital platforms such as Messenger Kids or YouTube Kids, I ask how the service provider can ensure adults are not using these platforms posing as children. Although these platforms can be successful and shift the focus on carer-child interaction and understanding of the online world, are there precautions in place or precautions drafted to ensure that adults cannot pose as children on these platforms?

Risk & Education

Above all, I believe that the most comprehensive safety measures in the online world can be provided by carers and educators close to young people. Social media and digital tools are an inescapable aspect of daily life, and restricting access to social media or digital tools as a whole until the age of 18 reduces connection, cultural/educational exposure, and skill-building opportunities for young people. While platform and provider based protection measures such as filtering opportunities, parental controls, community guidelines and terms of service

enforcement can contribute strongly to a safe online space that reflects the purpose of the online platform, the most comprehensive online safety measure is education. Young people deserve to be taught and guided to become responsible, informed digital citizens.