Response to consultation

Consolidated Industry Codes of Practice for the Online Industry

20 November 2024

About Yoti

Yoti is a digital identity company that makes it safer for people to prove who they are. Founded in April 2014, we started by creating a secure Digital ID app which gives people a safer and instant way to prove their identity, with no need to show identity documents or share an excessive amount of personal data. Yoti now provides verification solutions across the globe, spanning identity verification, age verification, age estimation, eSigning and authentication. We're a team of over 400 people, working together to shape the future of digital identity.

We're committed to making the digital world safer for everyone. Our seven ethical principles guide us in everything we do and we're held accountable by our independent Guardian Council, whose minutes we publish. With an award-winning social purpose strategy, we're always looking for new ways to explore what (digital) identity means globally. The journey isn't one we're making alone, but with the help of policy advisers, think tanks, researchers, humanitarian bodies and everyday people.

What we are doing and why:

- Transforming the way individuals can prove their age and identity
- Increasing security and privacy of personal data
- Helping to create age-appropriate experiences and safer communities online
- Creating the most reliable and comprehensive identity verification solutions
- Shaking up the way we sign documents

Technology as a force for good - Yoti was founded on seven business principles which guide our actions. Yoti is also a founding UK B Corp, meaning we aim to balance profit with purpose.

Security credentials - We commission regular external audits of our business and have been certified to meet some of the world's most stringent security standards, such as ISO 27001 and SOC2 Type II. We are also certified by the UK Government under the UKDIATF (UK Digital Identity & Attributes Trust Framework)

A transparent, open and honest approach - Yoti publishes regular white papers to build trust and understanding of our technology.

General feedback

We regret that these Codes have seemingly been developed without any significant input from the age assurance industry, which results in a document that feels watered-down and unclear. There are a number of approximations and contradictions which we will highlight in our document, and we will make suggestions which we think would improve the degree to which all Australians are protected online.

When compared to policy and technical documentation published in Ireland, France and the United Kingdom among many, the Codes show a clear and worrying lack of ambition.

In particular, the Codes as they are now set a vague requirement for industry participants to implement age assurance. However, there are many caveats, and a general lack of clear objectives and technical requirements. Overall, this means that the implementation of credible age assurance to prevent Australian children from accessing harmful and age-restricted content is less likely, and it will soon become very obvious that Australia is on a different compliance trajectory than other like-minded and comparable countries.

Approach to age assurance

We agree with the statement that *'industry will have different age assurance capabilities, which may change over time as technology develops'*. This is why we will make a recommendation throughout our response that the eSafety Commissioner, not industry, should conduct regular audits of the various age assurance that are being deployed at scale on the market. These technical audits should assess the efficiency and effectiveness of those age assurance solutions, and the Commissioner should then make recommendations on which solutions it deems to be effective.

We will also repeat the following points throughout our submission. We believe that these reviews should occur more frequently than at the three year intervals as currently suggested in the document. They should instead take place on an annual basis, to account for the rapid pace of technological development and improvement, and the deployment of novel solutions on the market.

'Definitions and interpretation' section

The definition as currently laid out fails to account for the fact that age assurance is not always used to *'verify the exact age or age range of a given user'*. Age assurance can also be used to assess whether a user is below or above an age threshold, such as a minimum, legal age required to access content or purchase age-restricted goods and services.

We think the definitions of age verification and age estimation should be amended to reflect this fact.

Definition of *'Australian child'*

We would want to see this definition refined. In particular, we think it should clarify precisely what constitutes an *'Australian child'*. We would recommend ensuring that the definition makes no distinction between children holding Australian citizenship and those who do not. All children residing in Australia, regardless of their citizenship status, should be equally subject to Australian law and afforded an equal level of online safety and protection.

We note that the wording in the *'Online safety objectives'* section uses the term *'children in Australia'*, which conflicts with the above definition.

'Compliance' section

Our feedback will focus on section (c) (*'In determining appropriate age assurance measures for the purpose of this Code*)':

This section encourages industry participants to *'take into account the technical accuracy, robustness, reliability and fairness'* of an age solution. We think the document should go further and set numerical accuracy objectives and thresholds. In responses to other similar consultations, we have suggested that solutions should be audited, and meet high reliability and attack detection rates.

For instance, Yoti has been reviewed by ACCS and previously NCC Group, on behalf of the BBFC, and Yoti's liveness detection technology was also reviewed by the United States' National Institute of Standards and Technology (NIST). Yoti's 'MyFace' technology was awarded 'iBeta NIST Level 2' with 100% attack detection rate by NIST in 2023. In October 2025, ACCS independent testing reports 99.3% of 18 years are reliably estimated to be under 25 (a 7 year buffer), and that 97.8% of 18 year olds are reliably estimated to be under 21 (a 3 year buffer).

We think the word 'reasonable' should be replaced by the word 'effective'. This criteria of effectiveness should be tied to the numerical targets mentioned above.

We think industry participants should go beyond simply seeking *'to limit'* circumvention *'where reasonably possible'*. We have previously suggested that the eSafety Commissioner should conduct annual reviews of age assurance solutions deployed on the market. This annual assessment should also include the effectiveness of those solutions, and as part of this how easily they can be circumvented. This should be a consideration in the choice of an age assurance method.

Therefore, we are surprised to see the inclusion of 'credit card checks' in the list of *'age assurance measures that will be considered appropriate'*. First, this is because it will exclude a significant amount of the population and could breach a duty of equality. According to a report published by the Australian Senate[1], only 40% of Australians had a credit card in 2015. A July 2024 report by the Australian Securities & Investment Commission[2] showed that the number of credit cards in circulation in Australia had gone down from 14.1 million to 11.8 million.

Secondly, credit cards are notoriously easy to access, including by children without the knowledge of their parents. The argument that the parent may subsequently see that a credit card has been used for such a check does not stand. Not all parents will have access to instant banking notifications on their smartphones, and not all parents scan through every transaction when they receive a copy of their accounts. Even if they did, the child would have already accessed the harmful and/or age-restricted content.

---

[1] 'Overview of the Australian credit card market', website of the Parliament of Australia, available at: https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/Credit_Card_Interest/~/media/Committees/economics_ctte/Credit_Card_Interest/c02.pdf

[2] Credit card lending in Australia: Staying in control, Australian Securities & Investments Commission on 30 July 2024, available at: https://asic.gov.au/about-asic/news-centre/news-items/asic-report-finds-credit-card-debt-still-a-pain-for-many-australians/

In its recent *'Protecting children from harms online consultation'*, UK regulator Ofcom flagged that a significant percentage of parents admitted lying, or assisting their children in lying about their age to access content and services that are age restricted. Therefore, we would welcome more detail on how the system of *'attestation by a parent or guardian of age'* should function. In our recent consultation response to the Children (Social Media Safety) Bill 2024, we recommend further consultation with civil society organisations to ensure that the legislation adequately reflects the diverse family arrangements present in Australia. Moreover, it would be helpful for the Bill to specify the processes deemed sufficient for an individual to prove they can provide consent on behalf of a child.

We welcome the recognition in this document that methods relying on self-declaration and contractual restrictions may not be considered appropriate. This is a view that is supported by a very large number of regulators and governments across the world.

It raises concern to see the document state that *'it may be reasonable for an industry participant to adopt no compliance measures'.* We have made suggestions below about the risk assessments that we believe industry participants should carry out.

'Process to identify compliance measures' section

We would like the addition of a duty for providers to publish and share their risk assessments with the eSafety Commissioner, in addition to notifying of *'the risk profile it has assigned'*. This would ensure that the regulator has access and can audit without having to go through the process of requesting these assessments, streamlining the process and ensuring quicker process.

We are concerned by the note suggesting that industry participants will not have to automatically notify the eSafety Commissioner that they have assessed their service *'falls within the exempted category and the reasons for making this assessment'*. We believe that there should be a duty on industry participants to notify the Commissioner, as such an assessment would mean that they would not put any age assurance measures in place. There is therefore much greater risk for children in an industry participant wrongly assessing that their service is exempt, rather than selecting the wrong risk profile.

We would like to see a set, numerical time limit for industry participants to provide *'reports relating to technical feasibility and practicability'* to the Commissioner.

'Code administration' section

We find the time periods suggested in (a) and (b) unreasonable. In effect, it means that the Code will not seriously be seriously enforced for a full calendar year following its publication.

By contrast, the UK regulator has said that their codes would be enforceable immediately, and the French regulator has said that the codes would be enforceable three months after publication, with only a further three months transitional period being granted to industry participants.

We repeat our point that *'records of the compliance measures'* industry participants adopt should be shared with the Commissioner and made available to the public.

We welcome the provision that ensures Australian end-users should be able *'to make a complaint to an industry participant about the industry participant's compliance with this Code'*. We think end-users should also be able to raise a complaint with the eSafety Commissioner, and we think the Commissioner should have a right to oversight of complaints received by participants.

We would strongly advise against implementing a three-year review cycle. Instead, we recommend an annual review cycle, especially of *'developments, including technological'*. Given the rapid pace of innovation and deployment in age assurance technologies, an annual review will be far more effective in keeping the Code up to date and relevant.

We question why these review cycles should include confidential consultations with the eSafety Commissioner. Instead, we think that all proceedings should be made public, and that contributions from members of the public, as well as age assurance industry professionals, should be invited.

Finally, we think reviews should be by the regulator, with the input of industry participants, members of the public and other relevant stakeholders.