From: [redacted]
To: OAIC - COPC
Subject: Feedback
Date: Friday, 5 June 2026 7:03:17 PM

Greetings to the members of the OAIC team that are creating the code.

My name is [redacted], I am a year 8 student and I am writing this to you in regards towards the new code about child privacy and how personal information should be handled.

I would like to share my feedback towards the newly proposed rules that are under consultation.

Privacy Advocacy and Personal Experience

I am all for children's privacy as I believe kids should have the ability to fully control what information that a site is allowed to take from you. I think this is great that this code focuses on this. I have had numerous instances where websites have confusing designs and layouts, which made finding the buttons to toggle off personal information is basically impossible. These confusing designs force kids and teens to give up or be limited to what information they can restrict from the website or platform accessing. I absolutely love what the OAIC are currently advocating for. It's great seeing so much effort being put for our safety. Now I want to talk primarily about rule two of your draft code.

Analysis of Rule #2:

While I was reading your 15 suggested rules that indicate what a website has to do to be compliant with the code, I encountered something odd. I skimmed over rule number #2 which quote:
"To protect your personal information, online services might have to either give everyone better privacy protections or check your age".

Now on the surface, this seems like a great precaution to take. Online services must make sure they take the necessary steps to help protect your personal information by either having much more secure privacy protections or check your age so that they know how much data they are allowed to take from you. However, this raised an eyebrow for me.

The Biometric Dilemma, Security Risks, and the "Roblox Model"

This code aims to protect children's personal information which also (under Australian law) includes biometric data. Now I assume that checking your age will involve some AI technology such as the company Persona provides for platforms. This intrigues me as this code aims for children privacy protection while it also encourages companies to collect the biometric data of children for safety?

This creates a massive risk of your data getting leaked. A "Honey spot", where the biometric data of kids and teens is stored, will create an opportunity for malicious people

and hackers to target and access that sensitive data holding many people's faces hostage for a ransom. To prevent this, if age checks are used, the Code must mandate a strict "zero-retention" requirement for vendors, forcing the immediate deletion of raw biometric data upon verification with proof.

I strongly commend the inclusion of Section 8(4) (which is the official legal draft code), which mandates the destruction of sensitive information as soon as practicable after verification. However, the OAIC must ensure this is strictly enforced with zero loopholes, as private third-party vendors frequently find technical workarounds to retain data minimised tokens or metadata that can still be targeted by hackers for their profit.

The Code must actively discourage platforms from adopting intrusive models like Roblox's age verification system, which requires users to upload a government-issued ID alongside a live facial scan. Forcing kids to hand over highly sensitive government documents and facial biometrics to a third party vendor completely violates the principle of data minimisation. The Code also must prevent platforms locking down features which don't require active communication. Many companies have been locking features for users who haven't age checked, behind a wall that requires age verification to access. This creates pressure and the fear of missing out for the user pushing them to verify.

In the exposure draft code, Section 8(2) intends to create a 'risk-based approach,' large gaming and social platforms will weaponise the requirement for a 'higher degree of certainty' to justify intrusive Roblox-style data harvesting. Furthermore, Section 8(3), which allows platforms to collect personal information before ascertaining age if it's necessary for the check creates an immediate privacy vulnerability the moment a user lands on a site

This issue gets even more complicated when you look at how the Australian government is adding its own digital ID framework. While using a government digital ID is definitely safer than relying on random third party vendors, it still poses a massive risk. By linking everyone's biometric data to a centralised system, it creates a much larger, ultimate target for hackers. Instead of breaking into smaller individual websites, hackers will want to target the collective data of the entire network, putting everyone's safety at risk if the link is ever compromised. It is not a matter of how or why, it's a matter of when.

Not to mention how easily by passible the whole Age verification system is. And I got front row seats to see it live in action. My friend was easily able to bypass a video games age verification, specifically Roblox. To simply move up a higher age group, he pulled back his hair, wore our other friends glasses and tucked his cheeks, emphasising his jawbone. It worked, and he was able to gain access to the 16+ age group which had voice chat.

Systemic and Community Impacts

I understand that the aim of this method is to protect children's data, but this is not the way to go. There are many risks and safety issues that come with age verification softwares. Not to mention the absolute annoyance it causes for the communities on specific platforms where age verification has been issued. It's a total safety hazard for both communities and companies. In line with the Privacy Commissioner's guidance on proportionality, a Roblox style biometric check is completely disproportionate for general audience websites and should not be considered or encouraged.

My final thoughts

The OAIC should heavily prioritise and promote a 'Privacy by Default' pathway over age gating/verification. This 'Privacy by Default' mechanism is already legally structured within Section 8(5) of the exposure draft, which exempts entities from age-assurance if they apply children's protections to all end-users. The OAIC must actively encourage Section 8(5) as the primary gold standard for compliance, rather than treating it as an alternative exemption. The best outcome of this is if companies treat everyone's personal information like they are children or don't collect any information at all. This means corporations will have to change what data they collect and how much of it. This creates a systemic responsibility, which ensures that companies are putting actual effort into keeping data safe while not being able to harvest "too much" data from anyone.

Thank you for taking the time out of your day to read this, it means a lot to me that there are people advocating for the privacy and protection of kids and young teens. I hope you take my feedback into consideration when finalising your code. I preferred to send my feedback over mail than the preferred worksheets as this allowed me to express myself to the fullest of my ability. I would prefer if my name was hidden if my letter is displayed.