[redacted] [redacted]
**Subject:** Submission regarding the Draft Children's Online Privacy Code (Member of the public)
**Date:** Monday, 27 April 2026 11:32:03 PM



To the OAIC,

I am writing this as a member of the public and an IT professional with a background in network engineering and infrastructure. I have spent a lot of my time building and managing complex home networks and high end audio systems. Because of my work and my hobbies, I have a very good understanding of how data moves around and the risks involved with these kinds of systems.

I think the goal of protecting kids is fine, but the way this Draft Children's Online Privacy Code is written is a problem. It feels like it is moving us toward an internet where everything is blocked by default for adults.

The government talks about 72 million data points being collected on kids. I manage my own local servers and use open source tools specifically to avoid being tracked, so I know how bad advertising tracking can be. But trading a few cookies for facial recognition data is a terrible deal. You can delete a cookie or clear your browser, but you can't get a new face if that data gets leaked in a hack. Organizations like the EFF have been saying for a long time that making people verify their age is basically the same as ending privacy for everyone.

Section 8 of the draft says companies have to take "reasonable steps" to check a user's age before they even collect any personal info. If the only way to "reasonably" check someone's age is through a face scan or a government ID, how does that actually protect privacy? Isn't it just replacing one kind of tracking with something way more permanent and dangerous?

We have seen how dangerous centralization is. Look at the massive breaches we have already had in Australia with Optus, Medibank, and even Services NSW. If the government and the biggest companies in the country can't keep our data safe, why should we trust every "designated internet service" or school app to hold our biometric data? We even saw a leak of 70,000 Discord user IDs recently. If even the FBI's own email systems can get hacked, no one is safe.

Centralization is a single point of failure. Look at what happened with the CrowdStrike "glitch" that took down half the world's systems because everything was relying on one thing. By forcing everyone into a Digital ID system to verify age, you are just building a bigger target for hackers.

Section 13 of the draft says that for kids under 15, companies have to get consent from a parent and take "reasonable steps" to make sure that person actually is the parent. How is a website supposed to prove someone is a parent without collecting even more sensitive data on both the adult and the child? Doesn't this just create a massive database of family

relationships that hackers would love to get their hands on?

The timing is also very suspicious. This code starts at the same time the Digital ID system is being opened up to private companies in December 2026. It looks like the government is just trying to force everyone to use MyID. If every website has to check my age, then the "voluntary" Digital ID isn't really voluntary anymore.

I've seen how over-engineered systems usually fail. The social media ban from 2025 didn't work because kids just lie about their age anyway. Instead of making kids safer, you are just making things harder for adults. Now we have to give our ID or a face scan to random websites just to use the internet.

We should be looking at better ways to do this that don't involve a surveillance state. The internet should be treated like public infrastructure where we can move around without showing a passport at every single corner.

Regards,

[redacted]