

From: [REDACTED]
To: [OAIC - COPC](#)
Subject: Submission on Children's Online Privacy Code and under-16 social media enforcement
Date: [REDACTED]

CAUTION: This email originated from outside of the organisation. Do not click links or open attachments unless you recognise the sender and know the content is safe.

Dear Commissioner,

I am writing as an Australian parent and citizen who is deeply concerned about the trajectory of our children's privacy regime, particularly as it interacts with the proposed Children's Online Privacy Code and the new under-16 social media laws.[gov +4]

While I support genuine efforts to reduce harm to children online, I am alarmed by the emerging reliance on persistent identifiers, "age assurance" systems and broad "reasonable efforts" language, which risk normalising cradle-to-grave digital tracking of young people. This has the smell not of safety, but of quiet, bureaucratic tyranny.

1. Genuine opt-in from the start

Any collection or use of children's personal data beyond what is strictly necessary to deliver a service should be genuinely opt-in. That means:

- No default enrolment of children into data-intensive features or profiling.
- Clear, plain-language explanations to parents and young people about what data will be gathered, how it will be linked across services, and who it will be shared with.[gov +2]
- Explicit prohibition on platforms inferring or "constructing" children's profiles from adult data or shadow data where no opt-in has occurred.[sidley +1]

International practice shows that opt-in models for children's data, with strong rights to change one's mind, are both feasible and necessary to restore agency.[clarip +3]

2. Automatic opt-out and "hard sunset" at 16

If Australia is to maintain an under-16 framework, then the Code and associated legislation must include a hard sunset for any special identifiers or data regimes attached to children. In practical terms:

- On the day a young person turns 16, any "child" identifier used for age assurance or safety features should automatically expire and cease to function.
- Platforms must be prohibited from carrying those identifiers forward into adult profiling, behavioural targeting or risk-scoring.
- Young people at 16 should gain full adult rights to refuse further linkage of their historical child data, and to request deletion or de-linking of non-essential records.[gov +3]

Without this, we risk building infrastructure where the "child ID" simply rolls on into adulthood, enabling lifetime tracking under the banner of safety and convenience.

3. Restricting "reasonable efforts" and age-assurance creep

The current use of phrases like "all reasonable efforts" in enforcement discussions is dangerously elastic.[net +2]

If not tightly defined, it will inevitably be interpreted to justify ever-stronger age-assurance measures—government-linked IDs, biometric checks, cross-service data sharing—without corresponding limits on retention or repurposing.

I urge the OAIC to:

- Define "reasonable efforts" in a way that prioritises data minimisation and privacy by design, not maximal identification.[gov +3]
- Explicitly reject age-assurance schemes that depend on permanent, cross-service identifiers or linkages to government databases for routine online participation.
- Require that any age-assurance mechanism be temporary, purpose-bound, and incapable of being repurposed for policing, welfare compliance, or commercial profiling.

4. Addressing platform data "ownership" and legacy profiles

At present, platforms treat the detailed behavioural and relational data they hold on families as a commercial asset, created and controlled under long, opaque terms of service.[hriui +4]

New child-safety obligations must be paired with strong measures to prevent this data from becoming a permanent, unerasable record of a child's life.

I therefore recommend that the Code and related reforms:

- Clarify that children's personal information is not a corporate asset, and that any "ownership" or licensing

claim is strictly limited by the child's and family's rights under the Privacy Act.[gov +1]

- Impose default deletion or deep minimisation obligations on platforms when a child reaches the relevant age threshold, except where retention is strictly required by law.
- Prohibit the sale, transfer or use of legacy child data for targeted advertising or algorithmic profiling once the child hits the age threshold, unless they have explicitly opted in as an adult.[allens +3]

5. Upholding autonomy and avoiding a de facto national ID for children

The combination of under-16 bans, age-assurance, and permanent identifiers risks creating, in practice, a national digital ID system for children by stealth. This would fundamentally alter the relationship between young people and the state and between families and platforms.

Any child-privacy regime worthy of the name should have as its core goals:

- Allowing children to grow into autonomy and privacy, not permanent legibility to institutions.
- Ensuring that safety interventions are proportionate, temporary and reversible, rather than building permanent tracking tools.
- Maintaining a clear line between protecting children and constructing infrastructure that could easily be turned to social control in future.

I urge the OAIC, in finalising the Children's Online Privacy Code and advising on related legislation, to centre opt-in, automatic opt-out at 16, hard sunsets on identifiers, strong deletion rights, and strict limits on age-assurance technologies. These measures will help ensure that necessary efforts to protect children do not slide, unintentionally, into a system that parents and citizens rightly experience as tyrannical.

Thank you for the opportunity to comment. I would welcome ongoing public engagement and transparency as the Code and enforcement framework evolve.

Yours sincerely,

A black rectangular redaction box covering the signature of the sender.

Sent from my iPad