

Submission Opposing the Proposed Children's Online Privacy Code

To Whom It May Concern,

I write to strongly oppose the proposed Children's Online Privacy Code.

While protecting children online is an important and legitimate objective, this Code represents a disproportionate and ineffective regulatory response that raises serious concerns regarding privacy, anonymity, freedom of expression, data security, regulatory overreach, and the practical operation of online services in Australia.

Although the Code is presented as a privacy protection measure, many of its obligations can only be effectively implemented if online services first determine whether a user is a child. In practice, this creates a de facto age-verification regime that extends beyond existing age-restriction measures and applies to a broader range of online services and platforms.

This exposes a fundamental contradiction at the heart of the proposal. A Code purportedly designed to protect privacy may ultimately require the collection of additional personal information from users in order to establish their age. Rather than minimising data collection, the Code risks encouraging the collection and retention of sensitive information including identity documents, biometric data, facial scans, age-estimation data, and other personal identifiers.

The creation of additional repositories of sensitive personal information inevitably increases cybersecurity risks. Recent years have demonstrated that no organisation—public or private—is immune from data breaches. Australians have already witnessed major breaches affecting millions of individuals. Requiring more organisations to collect and store identity-related information creates attractive targets for cybercriminals and increases the risk of identity theft, fraud, and unauthorised surveillance.

The Code also threatens the longstanding principle of online anonymity. The ability to communicate, research, and participate online without revealing one's identity is not merely a convenience; it is an important safeguard for freedom of expression and personal safety.

Anonymous access is particularly important for:

- Journalists communicating with confidential sources.
- Whistleblowers exposing wrongdoing.
- Victims of domestic violence seeking support.
- Individuals researching sensitive medical conditions.

- Members of religious, political, or social minorities.
- Young people seeking information about personal or mental health issues.
- Citizens engaging in political discussion without fear of retaliation.

Any regulatory framework that effectively pressures platforms to identify users before they can access information or participate online risks undermining these important freedoms.

The Code also raises concerns regarding the implied freedom of political communication recognised within Australia's constitutional framework. While not an absolute right, Australians have a legitimate expectation that participation in public discourse will not become contingent upon identity verification or the surrender of personal information. Measures that chill lawful speech and participation deserve careful scrutiny.

Equally concerning is the lack of demonstrated effectiveness of age-verification and age-assurance technologies.

Despite significant political attention, there remains limited evidence that age-verification systems reliably achieve their stated objectives. Existing systems can often be circumvented through:

- VPNs and location-masking tools.
- False declarations of age.
- Shared or borrowed credentials.
- Overseas platforms operating beyond Australian jurisdiction.
- Alternative websites and services not covered by Australian regulations.

As a result, the burden of compliance falls overwhelmingly on law-abiding users, while determined users often continue to bypass restrictions with relative ease.

Age-estimation technologies themselves also raise significant concerns. Many systems are prone to inaccuracies, false positives, and false negatives. Such technologies may disproportionately affect individuals with disabilities, diverse ethnic backgrounds, or atypical appearances. The consequences can include wrongful denial of access, unnecessary collection of additional personal information, and discriminatory outcomes.

The Code risks creating a culture of precautionary over-compliance across the Australian internet ecosystem. Faced with uncertainty and potential regulatory penalties, organisations may choose to implement the most restrictive interpretation of the requirements. This can lead to excessive data collection, unnecessary identity checks, reduced access to lawful content, and barriers to participation for legitimate users.

The burden on smaller organisations should not be underestimated. Large multinational technology companies may possess the financial and technical resources required to implement complex compliance systems. Smaller Australian businesses, independent forums, community organisations, educational platforms, non-profits, and start-ups often do not. The result may be reduced competition, fewer services available to Australians, and increased market concentration in favour of dominant global platforms.

There are also significant concerns regarding regulatory creep. What is presented as a privacy framework appears capable of functioning as a secondary age-verification regime. Australians should be wary of identity verification requirements being introduced indirectly through regulatory codes and administrative mechanisms rather than through direct legislative debate and parliamentary scrutiny.

Once age-verification infrastructure is established, the temptation for future governments and regulators to expand its use is substantial. Systems initially justified for child protection may later be proposed for other categories of content, services, or online activities. This gradual expansion of surveillance and identification requirements has the potential to fundamentally alter the character of the internet in Australia.

The Code further risks normalising the principle that access to online information and services should be conditional upon proving one's identity or age. Such a principle is inconsistent with the open nature of the internet and risks eroding the presumption of privacy that Australians have historically enjoyed.

Importantly, there are alternative approaches that do not require widespread age verification or increased collection of personal information. Policymakers should prioritise:

- Digital literacy education.
- Enhanced parental tools and controls.
- User empowerment measures.
- Improved transparency from platforms.
- Strong enforcement against genuinely harmful and illegal conduct.
- Targeted interventions aimed at specific harms rather than broad population-wide verification systems.

These approaches address online safety concerns while preserving privacy, freedom of expression, and anonymity.

Protecting children online is a worthy objective. However, policy effectiveness must be demonstrated rather than assumed. Measures that impose substantial privacy costs on

millions of Australians should only proceed where there is clear evidence they will achieve their intended goals. To date, such evidence remains limited.

For these reasons, I urge the Office of the Australian Information Commissioner and the Australian Government to reject or substantially revise the proposed Children's Online Privacy Code.

Any framework intended to protect children online must strike an appropriate balance between safety, privacy, freedom of expression, anonymity, and democratic participation. The current proposal fails to achieve that balance and risks creating a less private, less open, and less secure internet for all Australians.

Yours faithfully,

A solid black rectangular box used to redact the signature of the sender.