Submission to Online Safety Consultation – Phase Two Codes

By [redacted]

Subject: Response to Proposed Social Media Age Restrictions under the Online Safety Amendment (Social Media Minimum Age) Bill 2024

Contact: [redacted]

Introduction

The Online Safety Amendment (Social Media Minimum Age) Bill 2024 is a step in the right direction but risks achieving more harm than good in its current form. While its intention to protect children online is commendable, the proposed measures are overly simplistic and disproportionately punitive, failing to address the nuances of a complex digital landscape.

Blanket restrictions won't stop harm; they'll push it into unregulated spaces. Small platforms face extinction under these penalties, while big tech barely flinches. The amendment sacrifices privacy in the name of safety, creating new risks instead of reducing them.

To achieve its goals, the amendment must shift from broad-brush penalties to precision policy by integrating smarter, fairer solutions that work for all stakeholders. Through tailored compliance, strengthened privacy protections, and parental involvement, we can build a safer digital environment without alienating users or stifling innovation.

Harms Caused by the Proposed Amendment

1. Negative Impacts on Smaller Platforms
   - Disproportionate Burden: The flat penalties of 30,000 penalty units fail to consider the operational and financial capacity of small-to-medium-sized platforms. These businesses often lack the resources to implement complex age-verification systems, potentially forcing them out of the market.
   - Stifling Innovation: Smaller platforms, many of which cater to niche communities or serve educational purposes, may cease operations due to compliance costs and risks of high penalties.

2. Insufficient Privacy Safeguards
   - Data Mismanagement Risks: Requiring platforms to collect and store sensitive age-verification data increases the risk of breaches, identity theft, or misuse by malicious actors. The amendment does not include clear guidelines on data minimisation or secure destruction.

- Intrusiveness: Intrusive mechanisms, such as uploading government IDs, can deter users and create additional risks if such data is mishandled.

3. Inadequate Addressing of Online Harms
- Overfocus on Age Restrictions: By limiting access based solely on age, the amendment fails to address broader issues such as exposure to harmful content, algorithmic manipulation, and the role of content moderation.
- Circumvention Risks: Children can easily bypass age restrictions by creating fake accounts or using anonymisation tools (e.g., VPNs), undermining the efficacy of the measures.

4. Alienation and Inequity
- Exclusion from Social Development: Adolescents (13–16 years) rely heavily on social media for peer interaction, cultural participation, and identity development. Blanket restrictions risk isolating them from their social circles, causing feelings of exclusion and rebellion.
- Reduced Parental Autonomy: The amendment removes discretion from parents and guardians, who are better positioned to decide when and how their children engage with social media.

5. Unfair Application of Penalties
- Ineffectiveness for Larger Platforms: For major platforms (e.g., Meta, TikTok), the flat penalty is negligible compared to their revenue. This reduces the amendment's deterrent effect and gives larger platforms a competitive advantage over smaller networks.

Proposed Improvements

1. Revised Penalty Structure

Introduce a sliding-scale penalty system based on platform revenue, user base, and level of non-compliance:
- Platforms with annual global revenue under $5 million AUD: Maximum fine of 1,000 penalty units.
- Platforms with annual global revenue between $5 million and $100 million AUD:
  - Base penalty: 2% of Australian revenue.
  - Additional penalties for repeated breaches: Public accountability measures (e.g., public notices or restrictions on ad targeting in Australia).
- Platforms with annual global revenue exceeding $100 million AUD:
  - Base penalty: 5% of Australian revenue or $10 million AUD, whichever is greater.
  - Additional penalties for repeated breaches:
    - Public reporting of non-compliance on government and platform websites.
    - Platform-wide visibility restrictions in Australia (e.g., throttling algorithmic content recommendations for non-compliant platforms).

2. Verified Parent/Guardian Discretion

Introduce a Parental Consent Framework to allow parents/guardians to grant access to age-restricted platforms for children under 16:

- Consent must be verified through secure processes, such as:
  - Linking to a verified parental account.
  - Submitting proof of guardianship alongside consent forms.
- Platforms must enable granular parental controls, allowing guardians to monitor and manage their child's activity.
- Require platforms to provide education resources for parents on managing online safety risks.

3. Government-Endorsed Digital Age Verification System (DAVS)

- Develop a Digital Age Verification System (DAVS) that:
  - Verifies user ages anonymously through tokens or hashed data.
  - Provides a standardised, privacy-focused solution for all platforms, reducing compliance costs.
- DAVS integration to be mandatory for large platforms, while optional (but subsidised) for smaller ones.

4. Strengthened Privacy Protections

- Mandate data minimisation practices:
  - Platforms must only collect data strictly necessary for age verification.
  - All verification data must be encrypted and destroyed within 14 days of account approval.
- Introduce regular privacy audits overseen by the Office of the Australian Information Commissioner (OAIC), with public reporting of results.
- Prohibit platforms from using age-verification data for advertising or algorithmic purposes.

5. Non-Monetary Penalties

- Public Notices of Non-Compliance: Published on the eSafety Commissioner's website and the platform's Australian homepage.
- Operational Restrictions: For repeated breaches, restrict platform visibility (e.g., content distribution) until compliance is demonstrated.
- Mandatory User Notifications: Platforms must notify all Australian users about their non-compliance and remediation steps.

6. Grant Support for Smaller Platforms

- Establish a Small Platform Support Fund to assist platforms with annual global revenue under $5 million AUD in adopting compliant age-verification systems:
  - Grants covering up to 80% of compliance costs (e.g., DAVS integration or equivalent).
  - Eligibility contingent on adherence to a simplified compliance framework.

7. Education and Awareness Campaigns
   - Fund national education initiatives to promote:
     - Digital literacy for children and parents.
     - Awareness of online safety resources and the amendment's goals.
   - Collaborate with schools to integrate digital safety into curricula.

Conclusion

The Online Safety Amendment (Social Media Minimum Age) Bill 2024, while well-intentioned, risks significant harm if implemented in its current form. The proposed measures disproportionately impact smaller platforms, fail to adequately protect privacy, and overlook the broader risks of online harm and exclusion.

To create an effective and equitable framework, I strongly urge the adoption of the proposed improvements in this submission. These include proportional penalties, a government-endorsed age verification system, strengthened privacy protections, and parental involvement. By addressing these gaps, we can achieve a balanced policy that protects vulnerable users without stifling innovation or overburdening businesses.

I look forward to seeing a revised and refined framework that aligns with these principles. Thank you for considering this submission.