Submission to the Senate Standing Committee on Environment and Communications Inquiry into the Provisions of the Online Safety Amendment (Social Media Minimum Age) Bill 2024

Submitted by CitizenGO Australia

About CitizenGO

CitizenGO is a global advocacy organisation committed to defending life, family, and freedom. Operating in over 50 countries, CitizenGO empowers citizens to influence public policy and protect fundamental rights through grassroots campaigns. In Australia, CitizenGO has maintained a focus on promoting privacy, freedom of speech, and the accountability of governments and corporations. We believe in safeguarding individual liberties while addressing societal challenges in a way that upholds democratic principles and respects personal dignity.

Introduction

This submission raises significant concerns regarding the provisions of the **Online Safety Amendment (Social Media Minimum Age) Bill 2024**. While the stated intention of the Bill is to protect young Australians from harm on social media, its provisions pose serious risks to privacy, freedom of speech, and democratic accountability. Specifically, the Bill grants disproportionate and unchecked power to the eSafety Commissioner, a non-elected bureaucrat, and establishes mechanisms that may lead to invasive data collection and the erosion of fundamental freedoms.

Key Concerns

1. Disproportionate Power Granted to the eSafety Commissioner

The Bill assigns significant discretionary powers to the eSafety Commissioner to interpret and enforce its provisions, including determining what constitutes "reasonable steps" for compliance.

- **Wide Discretion**: Section 27(1)(qa) empowers the Commissioner to unilaterally formulate guidelines for compliance. These guidelines are not legislative instruments, meaning they are not subject to parliamentary scrutiny or oversight.
- **Potential Ideological Bias**: The eSafety Commissioner has previously suggested that freedoms such as speech must be "recalibrated" against safety and security. Such a stance indicates a willingness to subordinate fundamental rights to subjective interpretations of "safety."

- **Unchecked Authority**: The Commissioner is authorised to investigate and enforce compliance (Sections 63G and 63J), issue penalties, and publish findings of non-compliance, potentially damaging reputations without judicial oversight.

Implications:

- A non-elected official holds the power to define and enforce compliance with vague statutory terms, creating the potential for overreach.
- Platforms may be compelled to adopt invasive measures to avoid penalties, leading to disproportionate regulation.

---

2. Privacy Risks: Collection and Use of Personal Data

The Bill requires platforms to verify users' ages using "reasonable steps," which may involve the collection of sensitive personal information such as government IDs or biometric data.

- **Mass Data Collection**: Section 63F allows platforms to collect and hold personal information for age assurance purposes, significantly increasing the risk of data breaches and misuse.
- **Biometric Scanning**: Although not explicitly required, the Bill permits platforms to adopt technologies like facial recognition, which would normalise the use of invasive biometric measures.

Implications:

- Australians' sensitive personal data could be exposed to cyberattacks or commercial misuse.
- Biometric data, once compromised, cannot be replaced, creating permanent vulnerabilities for affected individuals.

---

3. Erosion of Online Anonymity

The age verification measures required by the Bill inherently undermine user anonymity.

- **De-Anonymisation**: Age assurance systems link real-world identities to online accounts, creating a digital footprint that can be tracked or exploited by platforms, governments, or malicious actors.
- **Chilling Effect**: Individuals may self-censor or withdraw from online participation out of fear of being identified or penalised.

Implications:

- The Bill disproportionately impacts freedom of speech, particularly for individuals who rely on anonymity to engage in public discourse or share dissenting opinions.
- Anonymity is a critical safeguard for whistleblowers, journalists, and vulnerable communities, all of whom would face heightened risks under this Bill.

---

4. Ministerial Rule-Making Powers

The Minister for Communications retains significant discretionary power to define or alter the scope of the Bill through legislative rules.

- **Scope Expansion**: Section 63C(1)(b) allows the Minister to classify additional platforms as "age-restricted social media platforms" without primary legislative approval.
- **Exclusions**: Section 63C(6)(b) grants the Minister authority to exempt certain platforms, creating the potential for arbitrary or inconsistent application.

Implications:

- The broad rule-making power undermines the democratic principle of separation of powers and reduces transparency.
- Future governments could use these powers to expand the Bill's scope to include more platforms or services, normalising invasive practices.

---

5. Vague Definition of "Reasonable Steps"

The Bill fails to define "reasonable steps" for age assurance, leaving this open to interpretation by the eSafety Commissioner and individual platforms.

- **Inconsistency**: Different platforms may adopt varying approaches, leading to regulatory uncertainty and inconsistent user experiences.
- **Overreach by Platforms**: To avoid penalties, platforms may implement intrusive measures such as mandatory ID uploads or biometric scans.

Implications:

- Users could face unnecessary privacy invasions, and platforms might overcomply with the law at the expense of users' rights.
- The lack of clear standards undermines the transparency and fairness of enforcement.

---

6. Weak Oversight of Third-Party Data Processors

The Bill does not address how third-party vendors involved in age assurance should handle user data.

- **Data Sharing Risks**: Platforms may outsource age verification to external vendors, creating additional risks of data breaches and misuse.
- **Accountability Gaps**: There are no provisions regulating how third parties must store, use, or destroy the personal information they collect.

Implications:

- Australians' data could be mishandled by third parties with little oversight or recourse for affected individuals.
- The accountability framework is insufficient to protect users from the risks of third-party involvement.

Broader Concerns

The rhetoric surrounding this Bill echoes the tactics historically used by authoritarian regimes to suppress freedoms under the guise of "safety and security." Governments that prioritise "safety" over liberty often use this justification to suppress dissent, surveil citizens, and entrench power.

Also, if this Bill is truly about protecting children online, why is there no push for age assurance measures on pornography websites? These websites are arguably far more harmful to young people, yet they remain unaddressed while social media is being targeted. This discrepancy raises serious questions about the government's motives and the Bill's effectiveness in tackling real online threats to children.

Implications:

- The Bill creates a dangerous precedent where subjective interpretations of "safety" could justify broader restrictions on freedom and privacy.
- By normalising these invasive measures, the Bill risks undermining democratic principles and individual autonomy.
- The failure to address pornography websites while targeting social media undermines the government's credibility and highlights the Bill's flawed focus.

Conclusion

The **Online Safety Amendment (Social Media Minimum Age) Bill 2024** is fundamentally flawed and should be rejected in its current form. It poses unacceptable risks to the privacy, anonymity, and freedoms of all Australians by granting sweeping, unchecked powers to unelected bureaucrats and allowing invasive data collection practices.

The Bill has been rushed through Parliament without proper scrutiny, with a five-day inquiry and less than 24 hours for public submissions—this is no way to legislate on such critical issues. At the very least, a proper and extended inquiry must be conducted to thoroughly examine the significant privacy and overreach concerns raised by this legislation.

We cannot sacrifice the rights of all Australians in a misguided attempt to address the dangers of social media for children. This Bill is a threat to fundamental freedoms, and it must not pass as is.

George Christensen, National Campaign Director, CitizenGO Australia
Brian Marlow, Campaigner, CitizenGO Australia