Chair, Senate Standing Committees on Environment and Communications
PO Box 6100, Parliament House
Canberra ACT 2600
By email: ec.sen@aph.gov.au.

Cc: Tas Larnach, A/g Committee Secretary

22 September 2025

Dear Chair,

We write in response to the communication dated 29 August 2025 inviting X to make a submission by 22 September 2025 regarding the Senate's inquiry into the Internet Search Engine Services Online Safety Code and the implementation of the under 16 social media minimum age pursuant to the Online Safety Amendment (Social Media Minimum Age) Act 2024 ("Social Media Minimum Age").

We thank you for the invitation to share our views on the topic and reiterate our opinion as set out in our submission of 22 November 2024 regarding the Online Safety Amendment (Social Media Minimum Age) Bill 2024.

Our mission at X is to promote and protect the public conversation. We believe X users have the right to express their opinions and ideas without fear of censorship. We also believe it is our responsibility to keep users on our platform safe from content that violates our Rules. Violence, harassment, and other similar types of behavior discourage people from expressing themselves, and ultimately diminish the value of global public conversation.

X, as a platform, is *not* widely used by minors, currently has no lines of business that actively target minors, and does not allow advertisers to target minors. Known under-16 users in Australia represent approximately less than 1% of our Australian user base and significantly less again of our global user base.

Our content moderation systems are designed and tailored to protect users without unnecessarily restricting the use of our service and fundamental rights, especially freedom of expression. Content moderation activities are implemented and anchored on principled policies and leverage a diverse set of interventions to ensure that our actions are reasonable, proportionate and effective.

To enforce our Rules, we use a combination of machine learning and human review. Our systems are able to surface content to human moderators who use important context to make decisions about potential violations. This work is led by an international, cross-functional team

with 24-hour coverage and the ability to cover multiple languages. We also have a complaints process for any potential errors that may occur.

While X agrees that robust strategies for mitigating the risk of harm to children are fundamental, we advocate for a balanced approach which protects children without compromising their privacy, freedom of expression and access to information. Our concerns remain: protecting and balancing those rights should be integral to online safety, and not subordinated.

Further, we have serious concerns as to the lawfulness of the Social Media Minimum Age, including its compatibility with other regulations and laws, including international human rights treaties to which Australia is a signatory. We are especially concerned about the potential negative impact that the Social Media Minimum Age will have on the human rights of children and young people, including their rights to freedom of expression and access to information, principles which are enshrined in international treaties including the UN Convention on the Rights of the Child and the International Covenant on Civil and Political Rights, and which must be protected. These concerns are shared by leading human rights organisations including your own Australian Human Rights Commission[1].

The imposition of age assurance as a mandatory safeguard for protecting minors online is disproportionate in numerous contexts, particularly where providers of online platforms can deploy less intrusive, targeted tools and features that effectively enhance minors' safety and security without compromising user privacy or accessibility. These alternatives, widely implemented across major platforms, include empowering parents and guardians with granular controls while leveraging platform-level moderation to mitigate risks such as exposure to unsuitable or sensitive content, unwanted interactions or excessive screen time, allowing each family to customize parental controls to meet their needs. Beyond platform-specific implementations, broader risk-based strategies — such as holistic content moderation, default opt-outs for behavioral advertising to prohibit age-inappropriate promotions, and scalable protections for features like live streaming — ensure platform-wide safeguards that prioritize rapid enforcement over universal age gates, and further underscore the availability of privacy-preserving alternatives that address harms through design choices and user empowerment, rather than universal age bans. By prioritizing such measures, platforms not only comply with evolving regulatory expectations but also cultivate safer digital ecosystems tailored to diverse family needs, rendering age assurance an unnecessary escalation in most scenarios.

Further, there is no evidence that banning young people from social media will work as a comprehensive solution to protect young people online or reduce harms without creating new ones. Instead, available data from policy trials, scoping reviews, and expert analyses point to significant enforcement challenges, evasion risks, potential unintended consequences, and only marginal benefits.

[1] https://humanrights.gov.au/about/news/proposed-social-media-ban-under-16s-australia; https://www.amnesty.org/en/latest/news/2024/11/australia-must-efectively-reglate-social-media-than-ban-children/

Not least amongst these concerns is the risk that when minors are barred from mainstream, regulated social media services, they will migrate to less moderated or entirely unregulated alternatives, thereby exposing them to greater potential harms including privacy breaches or unmoderated content. These alternatives include services that enable end-users to communicate with each other by means of messaging, and services that enable end-users to play online games with others, where safety features and content moderation are absent or inadequate, thereby exposing them to amplified risks, where controls are not as robust as consolidated social networks.

In addition, strict age bans carry significant evasion risks due to technological limitations, user ingenuity (with a mix of low-tech and high-tech strategies to evade restrictions, often with minimal effort), and enforcement challenges. Virtual private networks (VPNs) are widely available to the general public, and, short of a blanket prohibition or the adoption of disproportionate, invasive, and costly technical measures, there are no effective means to prevent their use as a potential circumvention tool for the age ban. Similarly, parents or siblings could readily create accounts on behalf of minors or share accounts and/or devices with them, a scenario over which providers have very limited ability to exercise meaningful control.

Regulators should prioritize strategies promoting age-appropriate features across regulated platforms, raising awareness of vetted safer alternatives, and fostering international regulatory coordination to ensure consistent protections across digital ecosystems, enhancing enforcement through layered, privacy-focused approaches rather than relying solely on bans.

International regimes have considered the current 13+ age as appropriate for social networks. We further note that the Joint Select Committee on Social Media and Australian Society did not include a ban in its recommendations and more than 100 experts in the Australian Child Rights Taskforce have opposed the ban in a letter to Prime Minister Albanese, with concerns that it risks isolating young people, preventing them from accessing mental health support and making social connections.

The Social Media Minimum Age introduced a new definition of *'age-restricted social media platforms'*, which is expressly intended to "*...cast a wide net...*", whilst at the same time providing flexibility to reduce the scope or further target the definition through legislative rules made by the Minister for Communications, having regard to advice from the eSafety Commissioner, or other relevant Commonwealth agencies. This approach brings with it a significant risk of regulatory weaponization, as the Minister for Communications will have broad discretion to define age-restricted social media platforms without any clear or objective criteria. This poses a major threat to freedom of information, speech, and access to the internet.

We would also submit that the Social Media Minimum Age is setting up a punitive regime. This singular focus on social media platforms promotes an adversarial approach and fails to incentivize parents and caregivers to take responsibility for the online activities of the young people in their care. It places the entire burden on social networks to resolve an issue that actually demands shared responsibility and deep cooperation across the whole of the technology ecosystem, including device manufacturers and app stores, governments, families,

and society as a whole.

We would encourage far deeper consideration be given by the Australian government to age assurance mechanisms at the device or app store level, as the most effective and privacy protective solution to protect young Australians from accessing inappropriate content online. These entities are uniquely positioned as gatekeepers to the online ecosystem, being able to provide downstream platforms such as X with signals about a user's age, which could significantly aid age assurance while protecting privacy and unburdening online participation.

For instance, device manufacturers often collect date-of-birth information during account creation, enable parental controls or family sharing features that flag child accounts, and use payment methods like credit cards as implicit adult indicators. App stores similarly gather age-related data through user profiles, app download restrictions based on content ratings, and verifiable parental consent processes for minors. Correspondingly, they could supply social media platforms with privacy-preserving signals, such as anonymized age ranges, digital tokens confirming parental consent without revealing full birth dates, or API-based flags indicating whether a user meets age thresholds—all while minimizing data exposure.

Compelling their cooperation, as seen in emerging U.S. state laws requiring app stores to handle age assurance for downloads, could deliver scalable, privacy-preserving solutions that enhance protections, reduce friction for users, and ease access to online services across ecosystems.

X is committed to continued collaboration with industry in this area because we think that device or app store level age assurance could provide global, scalable solutions which preserve privacy, improve user protections and reduce significant obstacles to people accessing online services.

As far as privacy rights are concerned, age verification is contrary to appropriate data minimization principles, which mandate reducing the amount of data collected in the first place, to the extent it is possible, to reduce consequent risk. This has a greater impact since establishing a social media minimum age would require not only the collection of data of teenagers, but data from virtually all users of the platform, potentially including the collection of sensitive information such as government IDs or biometrics like face scans.

As far as privacy rights are concerned, the consent obligations set out in section 63F of the Social Media Minimum Age appear to go beyond those that would otherwise be required under current Australian privacy law. The collection and use of age information would likely only be a matter of notice, not consent, under current privacy law, whilst the matters set out in Section 63F(2) of the Social Media Minimum Age, whilst these may be considered best practice, are at least arguably not matters which are formally embedded in Australian privacy law. This creates a potential issue where personal information is used by platforms both for age assurance/verification as well as for broader purposes (such as content management, targeting of advertising etc).

The Online Safety Amendment (Social Media Minimum Age) Act 2024 does not fully clarify *how* platforms must comply with the Social Media Minimum Age obligation, but rather requires that platforms take *"reasonable steps to prevent age restricted users having accounts with the age*

restricted social media platform". It provides no specific instruction on what constitutes "*reasonable steps*", instead delegating responsibility to the eSafety Commissioner to issue written guidelines to guide industry on how to fulfil that obligation.

For industry, receiving these guidelines from the eSafety Commissioner is absolutely critical, as platforms cannot effectively plan compliance measures without clear definitions of "reasonable steps". Once issued, industry participants require sufficient lead time for review, assimilation, and implementation, particularly given the potential need for substantive engineering changes, such as integrating age assurance technologies, updating detection systems, and ensuring scalable enforcement.

Companies are required to comply with the Social Media Minimum Age by 10 December 2025, yet the guidelines were only issued by the eSafety Commissioner on 16 September 2025. This leaves industry with mere weeks to interpret, plan, and deploy compliance measures under the threat of substantial penalties, exacerbating risks of incomplete implementation, higher costs, and potential inconsistencies across platforms.

The lack of earlier clarity and resulting uncertainty stemmed from a sequence of delayed actions:

The Online Safety Amendment (Social Media Minimum Age) Act 2024 was passed by Parliament on 29 November 2024, receiving royal assent shortly thereafter on 10 December 2024, with platforms required to comply by 10 December 2025. The final report from the Australian Government's technical trial of age assurance technologies to assess their effectiveness, maturity, and readiness (the "Age Assurance Trial"), which was announced on 14 May 2024, was only published on 1 September 2025. The supporting Online Safety (Age-Restricted Social Media Platforms) Rules 2025 - specifying exemptions for certain services - were not made until 29 July 2025. Finally, the eSafety Commissioner was formally instructed to prepare regulatory guidance and advice on June 19, 2025, with eSafety's stakeholder consultation on implementation commencing in June 2025 (following a public call for input on May 5, 2025), and X being invited to participate on August 12, 2025, with the guidelines then published on 16 September 2025.

Given the technical nature of the solutions expected in such guidance, X considered it essential that eSafety's consultation process included an opportunity for industry to review and provide feedback on an actual draft of the guidelines. Regrettably, no draft was provided for advance consultation, limiting meaningful input from industry on the guidelines.

We also note that the Office of the Australian Information Commissioner has not taken any formal position in this framework.

We therefore respectfully submit that the timing of any compliance obligation should commence a reasonable period - such as at least six months - *after* the issuance of the regulatory guidelines, following targeted consultation on those guidelines (contrary to what occurred in practice). Additionally, a grace period should be incorporated to allow adequate time for companies to implement what may involve complex engineering changes, thereby promoting effective compliance, reducing unintended harms, and supporting innovation in online safety.

Compounding these challenges is the registration on 9 September 2025 of the Social Media Services (Core Features) Online Safety Code (Class 1C and Class 2 Material) and Social Media Services (Messaging Features) Online Safety Code (Class 1C and Class 2 Material), which impose separate age assurance requirements for social media platforms to restrict access for users under 18 to specific categories of content (the “Phase 2 Codes”). While the Social Media Minimum Age focuses on preventing the holding of accounts entirely by users under 16 years old, the Phase 2 Codes require platforms to implement additional age gating for specific content within services, leading to parallel, overlapping obligations that demand consistency in age assurance technologies and processes to avoid inefficiencies, user confusion, and redundant compliance efforts. Regrettably, the simultaneous rollout of these frameworks without harmonization risks inconsistent standards, heightened administrative burdens, and fragmented enforcement, underscoring the need for better regulatory alignment to ensure cohesive online safety measures.

The above serves to further highlight the complex regulatory burden that social media networks are subject to under the current Australian framework. The Australian Online Safety Act 2021 (OSA) has engendered a lamentably layered and excessively complex regulatory regime. It is characterized by an array of overlapping voluntary expectations, industry codes, and statutory standards, which sit alongside existing privacy, telecommunications, and other applicable laws and regulation, at both Federal and State level, which leads to conflict as well as compliance and administrative inefficiencies, ultimately undermining the Act's objective of fostering a safer digital environment. The fragmented architecture - dividing the online sector into eight subsections - exacerbates uncertainty and leads to heightened and excessive compliance costs that disproportionately affect smaller or emerging providers. It requires wholesale simplification, to transform the OSA from a cumbersome patchwork into an agile, effective framework that truly prioritizes end-user safety without extraneous complexity.

A balanced approach is the only way to protect individual liberties, encourage innovation and safeguard children.

Yours sincerely,

X Corp.