Australian Information
Industry Association

Australian Information Industry Association

Submission on the

Internet Search Engine Services Online Safety Code

22 September

aiia.com.au

Introduction

The Australian Information Industry Association (AIIA) welcomes the opportunity to provide input to the Senate Environment and Communications References Committee inquiry into the Internet Search Engine Services Online Safety Code.

We support efforts to protect children and young people online while also ensuring that any regulatory measures remain evidence-based, proportionate to risk, and technically feasible. The AIIA's submission focuses on two key themes:

1. The importance of risk-based, proportionate age assurance requirements as an enabler of safer online experiences.

2. The distinctive nature of search engines compared to social media and other platforms, and their unique role in the information ecosystem and the public's expectation of privacy and anonymity.

3. The need to complement regulatory approaches with education and parental empowerment, enabling children and parents to make informed, values-based choices and build lasting digital resilience.

Our goal is to provide constructive recommendations that enable Parliament, the eSafety Commissioner, and industry to work together to achieve a balanced regulatory framework that protects children, respects users' rights, and fosters ongoing innovation.

Contextual and Proportionate Age Assurance

Age assurance techniques should be viewed as a means to create age-appropriate experiences for users, rather than a silver-bullet solution for online safety. In practice, obtaining reliable information about a user's age is valuable only insofar as it is used to tailor that user's experience to what is age-appropriate and safe. The primary question for policymakers and industry is how better data on user age can enable more effective safety measures in ways that are proportionate to the level of risk on a given service.

The Government's recent Age Assurance Technology Trial report[1] demonstrated that a wide range of age assurance approaches exists, including official ID checks, AI-based age estimation, and inference from user behavior, each with different strengths, weaknesses, and use-case suitability. The report explicitly concluded that "there is no one-size-fits-all solution"[2] to age assurance; rather, multiple effective technologies can be employed and should be matched to the context and risk profile of the service. Just as online services

[1] Australian Government, Age Assurance Technology Trial – Final Report, 2025.
[2] Ibid., p.15.

vary greatly in how they operate and the risks they pose to children, so too should age assurance measures be tailored to fit those differences. A social media platform with extensive user-generated content and high interaction among strangers presents very different risks compared to, say, an educational website or a search engine. The age assurance methods and stringency appropriate for one may not be appropriate for another.

We support the development of clear guidelines on what constitutes acceptable age assurance under the Phase 2 Industry Codes. In doing so, it is essential that the eSafety Commissioner's guidance incorporate the key findings of the Government's trial and industry consultations. We urge that any guidance or standards remain principles-based and flexible, allowing providers to use a range of age assurance tools (and combinations thereof) that best fit their service model and risk level. Importantly, this approach will encourage innovation and improvement in age assurance technologies over time, rather than locking industry into a narrow solution. Providers should be empowered to adopt methods proportionate to their service's risk profile. For lower-risk contexts or where a service has other strong mitigations, a lighter-touch age gating approach may suffice; conversely, higher-risk services will need more robust assurance. The guidance should explicitly allow different approaches for different service types, rather than mandating the same method across the board.

A key element of a proportionate approach is strict adherence to the principles of data minimisation and proportionality. Age assurance must not result in the routine collection or retention of excessive personal information, such as biometric identifiers, scans of government-issued identification, or payment records, where these are not strictly necessary. The creation of new stores of highly sensitive data would introduce significant privacy and cyber security risks that could outweigh the intended safety benefits. Where possible, age assurance should be decoupled from identity verification. Users should be able to prove that they meet a minimum age threshold without disclosing their full identity or providing documents unnecessarily.

The Unique Nature of Search Engines

Search engines play a unique role in the information ecosystem and they differ fundamentally from social media or other online platforms in ways that are highly relevant to online safety and regulatory policy.

- **Search engines are not content hosts**. Rather, a search engine's core function is to help users find high-quality third-party web content relevant to their queries. They index publicly available third-party content and return links in response to user queries. Search engines do not host or publish user-generated content, distinguishing them from platforms like social media. Search engines operate by temporarily caching information to facilitate transmission, aligning them more with caching services than hosting services.

- **Search can be classified as a gateway, not a destination**. Users use search to reach other websites, reinforcing its role as a neutral conduit rather than a content curator.
- **Search is user-initiated and intent-driven.** Users actively input queries to find specific information, making search a tool for discovery rather than passive content consumption.
- **Search engines may surface particular content for valid reasons.** Search is often the first step in help-seeking step for users in distress or seeking health information. Users may seek out legal but sensitive or controversial content for research or educational purposes. Search engine systems are usually designed to connect users with what they're looking for, while ensuring that results are not misleading or harmful.
- **Privacy expectations are higher when using search.** Users expect to search anonymously without logging in or sharing personal data, unlike on social media platforms where an account is required to engage. Search engines usually only use search terms and contextual data (like location and language preferences) to improve relevance and do not engage in extensive personalisation or behavioural profiling, making it a lower vector for systemic data-related harms.
- **Search is not a social experience.** Unlike social media, search engines do not require user profiles or interaction, focusing solely on information retrieval. They do not allow users to post, share, or message others which significantly reduces the risk of user-to-user harm and systemic issues related to user-generated content.

Education and Parental Empowerment

Improving online safety requires more than regulatory measures; it also calls for investment in education and parental support that enables safer, more informed participation online.

Early digital literacy education in schools is critical to equip young people with the skills to navigate online spaces safely and think critically about the information they encounter. By integrating these topics into school curricula, children can build resilience and develop habits that support safe and responsible digital engagement over time.

Parents and caregivers also need access to clear, practical guidance to help them actively support their children's online experiences. Initiatives that provide coaching, accessible resources, and opportunities to develop their own understanding of digital risks will enable parents to play an active role in guiding children's use of technology.

Encouraging tools and approaches that promote open family dialogue about online behaviour will further strengthen a values-based approach to safety. Supporting conversations about acceptable use and healthy online habits fosters a culture of shared responsibility and informed choice, contributing to long-term, sustainable improvements in online safety.

Conclusion

The AIIA supports the Committee's efforts to examine how the Internet Search Engine Services Online Safety Code and related initiatives can enhance online safety for children. As this inquiry recognises, effective protection of children requires not only regulatory oversight but also a nuanced understanding of how different online services function and the varying risks they present.

Our submission urges the Committee to endorse a principles-based, risk-proportionate approach to age assurance, drawing on the Government's Age Assurance Technology Trial Report and allowing services to adopt solutions that best fit their context. The AIIA stands ready to continue engaging with the Government and the eSafety Commissioner to develop solutions that keep Australians safe online while preserving the benefits of an open, innovative, and globally competitive digital economy. Should you require further information, please contact Mr David Makaryan, Advisor, Policy and Media,

Yours sincerely

Elizabeth Whitelock
Interim CEO, AIIA

***

Australian Information
Industry Association

About the AIIA

The AIIA is Australia's peak representative body and advocacy group for those in the digital ecosystem. Since 1978, the AIIA has pursued activities to stimulate and grow the digital ecosystem, to create a favourable business environment for our members and to contribute to Australia's economic prosperity. We are a not-for-profit organisation to benefit members, which represents around 90% of the over one million employed in the technology sector in Australia. We are unique in that we represent the diversity of the technology ecosystem from small and medium businesses, start-ups, universities, and digital incubators through to large Australian companies, multinational software and hardware companies, data centres, telecommunications companies and technology consulting companies