22 November 2024

Australian Mobile Telecommunications Association (AMTA)
Communications Alliance
Consumer Electronics Suppliers Association (CESA)
Digital Industry Group Inc (DIGI)
Interactive Games and Entertainment Association (IGEA)

RE: Comments of ACT | The App Association, Draft Consolidated Industry Codes of Practice for the Online Industry (Class 1C and Class 2 Material) under the Online Safety Act 2021

ACT | The App Association appreciates the opportunity to provide input on the *Consolidated Industry Codes of Practice for the Online Industry (Class 1C and Class 2 Material)* under the Online Safety Act 2021.

I. Introduction and Statement of Interest

The App Association is a not-for-profit trade association representing the global small business technology developer community. Our members are entrepreneurs, innovators, and independent developers within the global app ecosystem who engage with verticals across every industry. We work with and on behalf of our members to promote a policy environment that rewards and inspires innovation while providing resources that help them raise capital, create jobs, and continue to build incredible technology. The app ecosystem, primarily propelled by the innovation of startups and small businesses, has surged in Australia, contributing significantly to the technology landscape. Valued at approximately AUD 2.5 trillion, this dynamic market has been instrumental in driving smartphone proliferation and fostering rapid growth within the technology sector. Australia is a robust player in the global app market and is consistently viewed by App Association members as a high-priority marketplace in which to participate. Over the last four years, revenue in this sector has surged by AUD 1 billion, servicing a user base of slightly over 20 million individuals.[1]

The global nature of the digital economy has enabled our members to serve customers and enterprises located around the world. As a result, our members routinely receive requests for data from law enforcement agencies, both within and outside of Australia. The companies we represent offer the unique perspective of small business innovators at the intersection of the global digital economy and government interest in accessing data for criminal investigations. Thus, the statutory review of the Act is directly relevant to our membership, and we appreciate the Commission's careful consideration of our views.

The App Association shares Australian policymakers' goal of creating a safer digital environment. The App Association commends aspects of the Online Safety Act that

[1] https://www.businessofapps.com/data/australia-app-market/#:~:text=Compared%20to%20its%20population%20size,the%20first%20half%20of%202023.

reflect priorities for risk-based, outcome-focused, and technology-focused approaches. The Act acknowledges the diverse nature of online services, allowing for flexibility in compliance measures while aligning obligations with the specific risk profiles of different services. We are generally concerned about the potential impact of the Online Safety Act on end-to-end encryption, adversely affecting on the privacy and security of end users. Additionally, we are apprehensive about the negative effect of these standards on the small business and app economy.

We appreciate the efforts of the Australian Mobile Telecommunications Association, Communications Alliance, Consumer Electronics Suppliers Association, Digital Industry Group Inc, and the Interactive Games and Entertainment Association in developing this code of conduct and for developing it in a transparent manner.

II. App Association Concerns on the Impact on End-to-End Encryption and Privacy of End Users

We reiterate concerns raised with Australian policymakers during the development of the Online Safety Act that its requirement for content detection without direct monitoring of private communications raises concerns about the practical implementation and effectiveness of compliance measures, especially for end-to-end encrypted services. The defining feature of end-to-end encryption is that no party other than the sender and the intended recipients, including the service provider, can access the contents. The imposition of a mandate to scan class 1A and 1B material would render it unfeasible for service providers to uphold their commitment to user privacy. It could compromise the fundamental principle of encryption. Moreover, any form of content moderation would likely involve the insertion of a backdoor or a system vulnerability. This could weaken encryption, leading to unauthorised access, exploitation, and surveillance.

In addition, the potential erosion of end-to-end encryption could create a disproportionate advantage for larger entities with the resources to comply with new regulations while maintaining user trust. Meanwhile, smaller businesses might struggle to navigate the trade-offs between compliance and maintaining their competitive edge based on privacy and security. In this regard, small app companies' interests are aligned with those of end users and children, who benefit immensely from the protections end-to-end encryption. The goal of facilitating investigation and content filtering must be weighed against the twin imperatives of empowering people to benefit from end-to-end encryption and fostering an environment conducive to innovation and growth. Sacrificing these latter aims in service of the former would result in a reduction in online safety for minors; undermined privacy and security protections for consumers, leading to undue financial and reputational harms; and weaker business prospects for small business innovators.

In cases of technical infeasibility, services must take appropriate alternative action. Although the Act does not mandate services to breach encryption, the alternative approach is not clearly defined, raising concerns about interpretation and potential privacy violations. Further, the Act's impact on encryption may disrupt the balance between online safety and user privacy rights. The challenge lies in addressing the

risks associated with harmful content while preserving the strong security and privacy that encryption provides users. Finding a balance will require careful consideration, transparency, and collaboration between policymakers, technology providers, and privacy advocates to ensure that online safety measures do not inadvertently weaken the essential protections offered by encryption.

III. Implications of the Online Safety Act on Small and Medium-Sized Enterprises (SMEs) and the App Economy

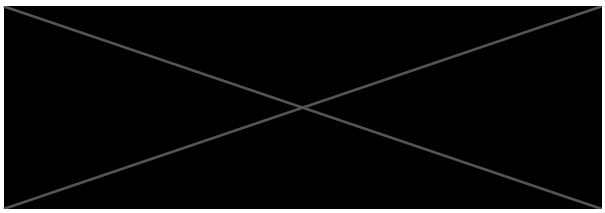
The potential impact of the Online Safety Act on encryption and online privacy can have serious consequences for small enterprises and the app economy. The Act increases business uncertainty, introduces barriers to innovation, and undermines the credibility of companies operating in Australia due to compromised digital security in their product and service offerings.

It is critical to emphasise that small business innovators would face more issues as SMEs and smaller apps often distinguish themselves by emphasising privacy and security as competitive advantages. If the Act requires compromising end-to-end encryption, it might erode users' trust in these smaller entities if their privacy measures are seen as compromised, leading to decreased adoption and usage. Larger companies might better weather the impact of compliance-related changes due to their resources and established user bases. Conversely, SMEs may need help adapting to new compliance measures. Implementing changes to adhere to the Act's requirements could be more resource-intensive for smaller entities, potentially diverting funds from innovation or growth. Stringent compliance requirements, especially if they involve compromising encryption, could discourage startups and innovators from entering the Australian market. The need to comply with these regulations might deter potential entrepreneurs from starting new ventures or introducing new services, stifling innovation and limiting competition. Australian businesses operating internationally may also be affected. If compliance with the Act's regulations affects the ability of Australian SMEs to compete globally, it might hinder their international expansion. Foreign customers might be wary of engaging with services perceived to have compromised privacy or weakened encryption. SMEs and startups that drive innovation and contribute significantly to economic growth could be forced to compromise their core privacy values, impeding the broader economic potential fuelled by their innovation and dynamism. The potential erosion of end-to-end encryption could create a disproportionate advantage for larger entities with the resources to comply with new regulations while maintaining user trust. Meanwhile, smaller businesses might struggle to navigate the trade-offs between compliance and maintaining their competitive edge based on privacy and security. Balancing regulatory requirements and fostering an environment conducive to innovation and fair competition will be crucial to sustaining a healthy digital economy that supports user privacy and business growth.

IV. Conclusion

The App Association appreciates consideration of the views above and welcomes the opportunity to further assist in creating a safe and secure digital environment.

Sincerely,



[redacted]
Senior Global Policy Counsel

[redacted]
Policy Counsel

[redacted]