

4 October 2024

Hon Stephen Jones MP
Minister for Financial Services
The Treasury
Langton Crescent
Canberra ACT 2600, Australia

RE: Comments of ACT | The App Association, Scams Prevention Framework exposure draft legislation

ACT | The App Association appreciates the opportunity to provide input to the draft implementing legislation of the Scams Prevention Framework.¹

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.²

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 governments' interest in protecting individuals from harmful online activity. Thus, the implementation of the Scams Prevention Framework 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. Our members depend on the trustworthiness of the wider online

¹ <https://treasury.gov.au/consultation/c2024-573813>.

² <https://www.businessofapps.com/data/australia-app-market/#:~:text=Compared%20to%20its%20population%20size,the%20first%20half%20of%202023>.

marketplace. If consumers are unable to trust that their interactions online are legitimate, they will be less likely to be willing to use products and services created by small and medium-sized developers. The App Association commends aspects of the exposure draft that encourage platforms and other entities to take reasonable steps to protect users from scams. However, we are concerned about the potential impact certain provisions could have on end-to-end encryption, which will have an adverse effect on the privacy of end-users.

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

The exposure draft proposes requirements that regulated entities identify consumers that have a higher risk of being targeted by a scam and take steps to detect scams as they happen. We are concerned that such requirements, when finalised, could force platforms to undertake actions that would undermine consumers' privacy and data security. If, for example, people in certain age groups are more likely to fall prey to scams than others, the requirement that regulated entities identify which of their users are more susceptible to scams could force them to collect more personal data than they otherwise would to facilitate age verification. We are also concerned that the requirement to detect scams as they happen could push regulated entities to collect more information regarding the content of private messages, even those currently protected by end-to-end encryption. 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 communications in real time to detect scams as they happen 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, who benefit immensely from the protections end-to-end encryption. The goal of protecting users from scams must be weighed in concert with 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; undermined privacy and security protections for consumers, leading to undue financial and reputational harms; and weaker business prospects for small business innovators. 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 Scams Prevention Framework for Small and Medium-Sized Enterprises (SMEs) and the App Economy.

The potential impact of the Scams Prevention Framework exposure draft on encryption and online privacy, if not carefully implemented, could have serious consequences for small enterprises and the app economy. The legislation could increase business uncertainty, introduce barriers to innovation, and undermine 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 final rules require 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 Framework'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 Framework'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 often drive innovation and contribute significantly to economic growth. If these entities face obstacles in complying with regulations without compromising their core privacy values, it could impede 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 foregoing views and welcomes the opportunity to further assist the Australian government in creating a safe and secure digital marketplace for consumers.

Sincerely,

A handwritten signature in black ink, appearing to read 'B. Scarpelli', with a stylized flourish at the end.

Brian Scarpelli
Senior Global Policy Counsel

Chapin Gregor
Policy Counsel

ACT | The App Association
1401 K St NW (Ste 501)
Washington, DC 20005
United States