13 December 2023

Executive Manager
Industry Regulation and Legal Services
Office of the eSafety Commissioner
PO Box Q500, Queen Victoria Building NSW 1230
Australia

RE: Comments of ACT | The App Association to the draft Designated Internet Services Standard and Relevant Electronic Services Standard for class 1A and class 1B material

ACT | The App Association appreciates the opportunity to provide input to the draft Designated Internet Services Standard and Relevant Electronic Services Standard for class 1A and class 1B material.

The App Association is a not-for-profit trade association for 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 for 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, consistently securing a place among Data.AI's top 20 markets worldwide. 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 a unique perspective of small business innovators at the intersection of the global digital economy and governments' interest in accessing data for criminal investigations. Thus, e-Safety's public consultation and the proposals contained therein directly impact our membership, and we appreciate the Commission's careful consideration of our views.

I. General Views of the App Association on the Online Safety Act (OSA) 2021

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

The eSafety Commissioner has proposed draft industry standards for the Online Safety Act 2021: the Relevant Electronic Services Standard and the Designated Internet Services Standards. The App Association shares e-Safety's goal of creating a safer digital environment. We appreciate the proposed legislative framework's aim to create a safer digital environment by regulating online platforms and services if the of government intervention outweigh its costs and wherever technically feasible. The standards seek to regulate harmful content categorised as Class 1A (e.g. Child Sexual Exploitation Material, Pro-terror Content) and Class 1B (e.g. Crime and Violence material, drug-related content) by implementing proactive measures, empowering end users and re-informing transparency and accountability in the online industry. We offer perspectives and recommendations below on the proposed scope of e-Safety's public consultation and surrounding issues and welcome the opportunity to assist e-Safety in its efforts moving forward to improve the draft industry standard.

The App Association commends the efforts by the Australian government to create a safer digital environment and we appreciate that the Online Safety Act adopts a riskbased, outcome-focused, and technology-neutral approach. It acknowledges the diverse nature of online services, allowing for flexibility in compliance measures while aligning obligations with the specific risk profiles of different services. However, we are concerned about the potential impact implementing these standards would have on end-to-end encryption, which may have an adverse effect on the privacy and security of end users. Additionally, we are concerned about the impact of these standards on the small business and app economy.

A. Online Safety Act 2021 Overview

The Online Safety Act 2021, which commenced on 23 January 2022, provides for the regulation of harmful online material by establishing new mandatory industry codes and standards for the five sections of the online industry to manage and prevent the distribution, production, and consumption of harmful online content classified as Class 1A and 1B (ranges from seriously harmful content such as CSEA material or acts of terrorism to online pornography). If a code does not meet the requirements, e-Safety can develop an industry standard for that section of the online industry instead. Further, it established new standards by introducing the Relevant Electronic Services Standard for electronic communication platforms and the Designated Internet Services Standard for services facilitating internet access and content delivery. Furthermore, it categorizes services by defining 'relevant electronic services' as encompassing communication platforms (e.g. email, instant messaging chat, dating services, and online games) and 'designated internet services', including various apps, websites, and online storage services.

B. Relevant Electronic Services Standard

The draft Relevant Electronic Services Standard set out requirements for providers of specified categories of relevant electronic services to proactively detect and remove known CSEM. These requirements apply to closed communication appropriate electronic services, including email and private online messaging services. E-Safety recognizes that some closed communication services,

particularly in an end-to-end encrypted environment, may face technical limitations in detecting known CSEM and known pro-terror material. Therefore, it applies only if it is technically feasible for the service to detect and remove the material. It does not require service providers to design systematic vulnerabilities or weaknesses into end-to-end encrypted services.

C. Designated Internet Services Standard

The Designated Internet service standard targets providers offering designated Internet services to end-users in Australia. This standard classifies service categories based on risk profiles, proposing proportionate and appropriate requirements for each category. The pre-assessed categories encompass tiers: Tier 1 includes high-impact services like 'gore' and pornography sites, Tier 2 contains services not in Tier 1 or 3, such as those offering professional and user-generated content, while Tier 3 covers services offering R18+ material. The standard includes General Purpose DIS, including educational, health, and news websites. A risk assessment methodology is outlined for services not fitting into pre-defined categories.

D. Proposed Compliance Measures

The Online Safety Act aims to implement proactive safety measures by creating and maintaining a safe online environment and empowering Australian users to manage their exposure to harmful content. Increase transparency and accountability among service providers regarding the presence and handling of class 1A and 1B material on their platforms. Adopt an outcomes and risk-based approach to compliance, ensuring that measures are proportionate to the risk level associated with different services while offering flexibility for implementation. This approach recognizes that different services and technologies may have different risk profiles. Compliance measures should be proportionate to the level of risk associated with a particular service and to the size and capacity of the service provider responsible for that online activity or service. Compliance measures should be flexible to enable effective implementation, recognize the differences between unique services, and adapt to technological changes and the risk environment.

II. The Proposed Draft Industry Standards Would Compromise End-to-End Encryption, Which Would Undermine Privacy and Security for End Users

The 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. By requiring service providers to access content their customers send or receive, the provision is plainly irreconcilable with end-to-end encryption. Moreover,

to detect and eliminate or reduce access to 1A or 1B content on an ongoing basis, a service provider would likely be forced to insert a backdoor or a systemic vulnerability.

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.

Failure to strike a balance between these equities could result in a requirement for service providers to access content they currently are unable to access. Such a mandate would weaken encryption, leading to unauthorized access, exploitation, and surveillance. Unfortunately, the result of creating vulnerabilities like these that did not previously exist would be enabling the kinds of grooming and exploitation the OSA seeks to reduce. Where children’s content and communications are currently protected by technical measures like encryption against access by predators, the proposed Draft Industry Standards would require those communications and content to be more accessible to predators. The ability to detect or interdict prohibited content in transit is unlikely to justify the imposition of new vulnerabilities that make it easier to exploit children and perpetrate crimes against them in the first place.

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

The potential impact of the OSA on encryption and online privacy can have serious consequences for the economy, especially for small enterprises and the app economy. If improperly implemented, the OSA would increase business uncertainty, thwart 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 than their larger counterparts by removing one of their key competitive advantages. SMEs and smaller app developers often distinguish themselves by emphasizing privacy and security as competitive advantages. If the OSA requires compromising end-toend encryption, it would erode users' trust in these platforms. Users might hesitate to trust 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 also raise barriers to entry for potential tech-driven startups. The need to comply with these regulations could deter potential entrepreneurs from starting new ventures or introducing new services, stifling innovation and limiting competition. International businesses may also be affected. If compliance with the OSA's regulations affects the ability of Australian SMEs to compete globally, it might hinder their international expansion. Foreign markets 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.

IV. Conclusion

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-toend encryption. The goal of facilitating investigation and content filtering must be weighed against the twin imperatives of empowering people to benefit from end-toend 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. Therefore, we urge that the relevant final Industry Standards avoid compromising end-to-end encryption.

Sincerely,

Brian Scarpelli
Senior Global Policy Counsel

Shanavi Dessai
Privacy Fellowship Manager

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