Friday November 12, 2021

The Hon Paul Fletcher MP
Minister for Communications, Cyber Safety and the Arts
Parliament House
Canberra ACT 2600
[redacted]

[redacted]
Department of Infrastructure, Transport and Regional Development and Communications
[redacted]

[redacted]
Department of Infrastructure, Transport and Regional Development and Communications
[redacted]

Dear Minister,

We are a diverse group of organisations representing a range of companies within Australia and internationally. We support the policy goals of online safety, and look forward to our continued work with you to advance those goals. We see the Online Safety (Basic Online Safety Expectations) Determination 2021 (BOSE) as a useful path to advance these discussions, and to drive greater uniformity and consistency in online safety. At the outset, we wish to emphasise that we agree with the Government's intentions.

However, we believe that elements of the drafting of the BOSE might actually serve to undermine its effectiveness in promoting online safety, and are also contrary to Australians' expectations of privacy and cyber security. We therefore write to express several key concerns with the determination, outlined below. We would like to work with you on these before the scheduled date of effect of the BOSE, in January 2022, in an effort to advance the broader policy.

Scope of services

Digital services covered under the BOSE include "designated internet services", which include every website or app that is accessible to Australian users, including those used in non-technology sectors and small business. "Relevant electronic services" includes all email, online messaging and gaming services, including text messages. "Social media services" is defined extremely broadly to capture services that enable online social interaction between two or more end-users.

We are concerned that the standards in the BOSE exceed the capabilities and capacities of the broad range of services that are caught in scope. As one example, Section 7 requires the providers of every single one of these services to individually seek the eSafety Commissioner's input on how they will meet these expectations. With a view to the Government's goal of Australia becoming a leading digital economy by 2030, the compliance burden of this initiative for different types of services must be critically examined.

The potential introduction of the BOSE in January 2022 does not provide all services in scope with due time to implement the yet to be finalised determination. The timeframe is especially challenging for small businesses that are devoting their limited resources to recovering from the economic impacts of COVID-19 and complying with related safety measures. To our knowledge, small business representatives were not consulted about the development of the BOSE; we ask you to reconsider the timeframe to enable that consultation. We would also urge the consideration of a more tightly applied scope, such that the need for businesses to take action against harms is proportionate to the risk.

Potential for over-cautious censorship

While we share the Government's goal that unlawful activity should be promptly addressed on relevant online services, we are concerned that the general expectation in Section 6 of the BOSE goes far beyond that expectation. It requires websites, messaging and digital services to address "potentially unlawful" and "potentially harmful" material. While many companies have terms of service to routinely restrict specified harmful material, those companies do not have certainty as to how the Government defines "potentially harmful" behaviour. Furthermore, Section 6 of the BOSE is not limited to matters concerning safety; it therefore overlaps with a whole range of existing laws concerned with non-safety related issues, such as copyright.

We are concerned that efforts to comply with these uncertainties in the BOSE will result in over-cautious censorship of content and legitimate speech that Australians may expect to be able to express in private and public conversations with their family and friends, as providers err on the side of caution in order to avoid any risk of non-compliance.

Potential for surveillance

Section 6 of the BOSE encourages the *detection* of "potentially harmful" and "potentially unlawful" content. We are unclear about how websites, messaging and digital services will be able to routinely predict this broad range of behaviour among their users. In practice, this incentivises proactive monitoring of users by services, which together with other provisions in relation to discouraging anonymity and encryption, can lead to privacy risks.

Specifically, Section 8 requires that service providers that use encryption within their services "implement processes to detect and address material or activity on the service that is or may be unlawful or harmful". There are major practical difficulties with this requirement, and we are concerned that this encourages service providers to avoid using encryption on their services altogether. Encryption is of foundational importance to Australians' cyber security. We welcome the Department's clarification in their FAQ on the BOSE that providers are not expected to monitor their users' private communications, and we ask that this be reflected in the legal instrument itself to provide business with legal certainty.

Potential for competition issues

Under the BOSE, all service providers must seek the guidance of the eSafety Commissioner on how they implement the determination. As well as the practical challenges noted earlier, it is concerning to us that this guidance is not required to be made public. If this guidance is provided to individual companies behind closed doors, then the broad range of websites, messaging and digital services caught in scope under the BOSE will have no confidence that the processes for determining and enforcing such guidance are consistent. Transparent guidance will help ensure a level playing field amongst competitors in the market, and inspire confidence that they are being treated fairly and have an equivalent compliance burden.

–

We believe that improvements in these areas will improve the effectiveness and operationalisation of the BOSE, as it will make the compliance obligations clearer for small and large companies alike.

All of our organisations believe in online safety, as well as privacy and cyber security. We believe there are ways to address our concerns with the BOSE without compromising the Government's commitment to online safety. To that end, our organisations are open to working constructively with you, your office and the Department to resolve these issues before the BOSE comes into force.

Sincerely,

Representatives of the following 11 organisations *(overleaf)*

Australian Information Industry Association (AIIA)	Asia Internet Coalition (AIC)	Communications Alliance (CA)
Council of Small Business Organisations Australia (COSBOA)	Developers Alliance	Digital Industry Group Inc (DIGI)
Global Network Initiative (GNI)	Interactive Games & Entertainment Association (IGEA)	Internet Association (IA)
Internet Association of Australia (IAA)	Information Technology Industry Council (ITI)	