21 February 2020

To the
Director
Online Safety Research and Reform Section
Department of Communications and the Arts
GPO Box 2154, Canberra ACT 2601

Subject: AIC Comments on Australia's Online Safety Legislative Reform - Discussion Paper

The Asia Internet Coalition (AIC) and its members express our sincere gratitude to the Department of Communications and the Arts ("Department") and the Government of Australia for the opportunity to submit comments on the Online Safety Legislative Reform - Discussion Paper ("Discussion Paper").

The AIC is an industry association comprised of leading Internet and technology companies. AIC seeks to promote the understanding and resolution of Internet and ICT policy issues in the Asia Pacific region. Our member companies would like to assure the Department that they will continue to actively contribute to the security of digital platforms, products and services in support of the digital economy goals of Australia. Our members are Airbnb, Amazon, Apple, Expedia Group, Facebook, Google, Grab, LinkedIn, LINE, Rakuten, Twitter and Yahoo (Verizon Media), and Booking.com.

We commend the Department for their efforts on drafting a new Online Safety Act **("Act")** to improve Australia's online safety regulatory framework. While we support these efforts to replace the existing framework with a single Online Safety Act, we express our concerns on some of the requirements proposed in the Online Safety Legislative Reform - Discussion Paper. As such, please find appended to this letter detailed comments and recommendations, which we would like the Department to consider when preparing the Online Safety Act.

We are grateful to the Department for upholding a transparent, multi-stakeholder approach in developing the Online Safety Act. We further welcome the opportunity to offer our inputs and insights, directly through meetings and participating in the official consultations.

Should you have any questions or need clarification on any of the recommendations, please do not hesitate to contact me directly at Secretariat@aicasia.org or +65 8739 1490. Thank you for your time and consideration.

Sincerely,

Jeff Paine
Managing Director
Asia Internet Coalition (AIC)

Enclosure

Detailed Comments on Australia's Online Safety Legislative Reform - Discussion Paper

I. Scope of proposed regulation

AIC would like to seek clarity around the scope of the proposed legislation. The proposed Act, which emphasises an all-of-industry approach, covers a wide range of online services including social media platforms, private messaging services and hosting services. We urge the Government to consider that risk of online harm and spread of illegal or harmful content is not the same across all online service providers.

We understand cloud computing to be largely out of scope of this proposed regulation. We agree with this as cloud infrastructure providers have no or little visibility of content stored on their hardware. The obligation to remove material should lie with the online service provider. In addition, we would also argue that the scope should not extend to hosting services that provide public cloud infrastructure services, where the provider is unable to identify, access or interdict material kept on its services by an online service provider. To that end, we would like to see the definition of "online service providers" be made clearer and more precise.

II. Basic online safety expectations

We would like to seek clarity on the basic online safety expectations (BOSE) scope, expectations and our obligations. The Discussion Paper underlines that the BOSE will be based on the Online Safety Charter and Safety by Design principles. It will be helpful to understand the interaction between these codes and principles, and which should take precedence.

Some aspects of these codes and principles are seemingly not aligned with the proposed legislation. For example, the proposed legislation requires all services marketed to children must default to the most restrictive privacy and safety settings at initial user set-up. However, item 2.1 in the Online Safety Charter states that "services should aim to provide technical measures and tools that adequately allow users to manage their own safety, and that are set to the most secure privacy and safety levels by default." There seems to be a disconnect between the Online Safety Charter relating to strictest defaults for all services, and the proposal to require strictest defaults for services marketed to children. We therefore recommend further clarity on this matter.

We understand that the Government will not impose sanctions for non-compliance of BOSE at this stage, but social media companies will be expected to report, through public transparency reports or directly to the eSafety Commissioner, on their actions in upholding these expectations. Transparency reports may serve multiple purposes – from alerting the broader community of activity on a service, to providing researchers data to study trends. However, any regulatory requirement to transparency reports should allow different services the latitude to design their own reports in a manner that would be appropriate for each service and determine the frequency of such reports.

Given the possible broad application of the BOSE reporting requirements (particularly over time), it will be essential that the implementation of the reporting obligations is sufficiently flexible to enable companies to comply in a manner consistent with their individual business practices and and the unique characteristic of their product and service.. Companies should have the freedom to apply terms, adjudicate specific facts, action reports, and change processes over time in ways that they believe best keeps their community safe.

AIC would like to strongly suggest that the Act also includes a "safe harbour" provision for companies who have made reasonable efforts to comply with BOSE and the reporting requirements, as well as built policies, processes and tools to quickly remove illegal or inappropriate online content or harmful conduct.

Lastly, the Act proposed to give the eSafety Commissioner power by legislative instrument to determine that BOSE apply to 'other specified types of service providers'. AIC considers this proposal to be contrary to the separation of powers doctrine that requires that only the Parliament can create a legal obligation upon an individual or entity. As such, any proposal to extend the scope of a legal obligation to additional parties should require a change to an Act of Parliament. The legislative instrument mechanism proposed in the Discussion Paper is an administrative act that operates not for a delegation of authority but to fulfil the administrative operation of an Act.

III. Cyberbullying scheme

We generally have no issue with the reduction to a 24-hour time period, as digital platforms respond to the vast majority of reports well under a 24-hour time period. However, we believe there should be exceptions where an investigation requires more time or there is a consideration of an appeal from the accused party.

We strongly object to having the eSafety Commissioner enforce a service provider's terms of use, This effectively allows a private company to create regulations that are enforced by the government, and perversely, could provide an incentive to companies to allow broader acceptable use policies because of fear that the government would require enforcement of stricter policies. Terms of use are often drafted broadly to capture a broad variety of cases, and companies may have more detailed internal enforcement guides (e.g. help to define what is "offensive" or "harmful"). The eSafety Commissioner would not have insight into the internal guidelines.

Specifically with regard to private communication such as email and other private messaging platforms, we recommend for it to be excluded given: (1) the nature of harm is different in private conversations versus public platforms; (2) these mediums generally have greater controls that individuals can use to protect their own safety; (3) there may be technical limitations in the ability to police harmful content on email and private messaging platforms.

IV. New cyber abuse scheme for adults

On extending the cyberbullying scheme to adults, we would like to stress that, as suggested in the Discussion Paper, it should only be limited to cases intended to cause serious distress or serious harm, and material regarded as menacing, harassing or offensive. We would also like to ask the Government to consider if further regulation is even needed in this area, given existing laws that may cover similar issues.

For Cloud Service Providers (CSPs), we wish to highlight that without precise and specific identification of an access URL to material that may be judged illegal or inappropriate or harmful, and an ability to access that URL, the only recourse a CSP would have were it to receive a takedown notice would be to shut down access to the entire customer account. The legal and material consequences of taking such action could be immense.

As mentioned in the previous section, while we do not object to the reduction to a 24-hour time period, we believe there should be exceptions where an investigation requires more time or there is a consideration of an appeal from the accused party. As for CSPs, it is completely inappropriate to apply those time frames to a CSP – which is further evidence of why CSPs should not be included in the scope of this Act.

As mentioned in the previous section, we strongly object to having the eSafety Commissioner enforce a service provider's terms of use.

V. Addressing illegal and harmful online content

We welcome an opportunity, as outlined in the Discussion Paper, to work with the eSafety Commissioner to develop a principles-based code for online service providers to address harmful content (Class 2 Content, under the Proposed Act). Through close consultation with industry, these codes can be flexible enough to account for the nature and characteristics of each online service provider.

We wish to highlight that the current and proposed online safety frameworks in Australia focuses on the mitigation of a range of harms that result from exposure to illegal or inappropriate online content or harmful conduct. It achieves this aim by providing the eSafety Commissioner with certain powers that are listed in the Discussion Paper. Those powers include, in relation to Abhorrent Violent Material (AVM) as defined in the Sharing Abhorrent Violent Material Act 2019, a power to issue to hosting service providers, including Cloud Service Providers (CSPs), a notice about the presence of AVM on their services.

The Sharing Abhorrent Violent Material Act 2019 creates a criminal offence for providers that do not expeditiously remove the material once they are made aware of its presence. The nature of AVM and its impact on society may justify this extraordinary power and claim to extraterritorial authority. However, Such a claim could not be comparatively made in respect of an individual harm that may be experienced as a result of exposure to illegal or inappropriate online content or conduct that is intended to harm an individual. There is also a risk that ordering takedown of such content hosted overseas may lead to a

conflict of laws, which can breach our individual companies' terms of service. An extraterritorial imposition of content hosted in Australia by a foreign state authority would likely not be welcome by Australia. Due to the above mentioned reasons, the same principles and objectives of Sharing Abhorrent Violent Material Act 2019 should not apply to Online Safety Act.

Specifically for CSPs, as the conduct or content that is the subject of this Act will be provided by services that are identifiable to the eSafety Commissioner, there is a clear avenue for statutory enforcement against those services that does not require the Commissioner to seek action by a CSP.

We also object to the proposed broad powers of the eSafety Commissioner to change the definitions of harmful content overtime. Such changes should only occur through a process of the Parliament.

We would also like to raise specific concerns about the apparent need for online service providers to proactively search for illegal content. While some platforms have extensive proactive searching efforts for particular types of content, it is not possible to proactively search for all content that could be illegal (eg. defamatory content) - especially since the definitions of content put forward in the discussion paper are so ambiguous. Importantly, many platforms have established regulator and law enforcement reporting channels and in-app reporting to help flag illegal and harmful content for review.

VI. Opt-in tools and services to restrict access to inappropriate content

The Discussion Paper proposes an Accreditation System for safety tools. We would like to request further information on how this would work in practice. For instance, which services would be required to submit safety tools for accreditation and what are steps involved in the submission and accreditation process?

If an accreditation system for online safety tools became overly prescriptive or standardised, it could be counterproductive. Instead, we believe that the Act should ensure that there's flexibility for different services to implement tools in ways that work for their particular products, particularly given the speed to which new products and product features are created at shorter cycles. The focus should be on ensuring tools are clearly communicated to consumers and achieve the safety objective in a way that works for the relevant product.

-End