The Australian Industry Group
[redacted]
Australia
ABN 76 369 958 788

12 November 2021

Director, Online Safety Reform and Research Section
Department of Infrastructure, Transport, Regional Development and Communications
Email: OnlineSafety@infrastructure.gov.au

Dear Sir/Madam

EXPOSURE DRAFT ONLINE SAFETY (BASIC ONLINE SAFETY EXPECTATIONS) DETERMINATION 2021

The Australian Industry Group (Ai Group) welcomes the opportunity to make a submission on the consultation with respect to the exposure draft of the Online Safety (Basic Online Safety Expectations (BOSE)) Determination 20201 (Draft Determination) by the Department of infrastructure, Transport, Regional Development and Communications (Department). We understand that this Draft Determination is aimed at setting out the online safety expectations the Government has for social media services, relevant electronic services and designated internet services.

Ai Group's membership comes from a broad range of industries and includes businesses of all sizes. Given the growing engagement across the business community with every business having the capability of having an online business or platform, we are particularly focussed on the implications for the broader cross-section of Australian businesses.

Overall, industry recognises the importance of protecting the safety and security of the Australian community, both in the physical and online realm. Indeed, Ai Group works closely with governments and their agencies on improving Australia's safety and security in a diverse range of areas. In this mix, the eSafety Commissioner has an important specific role to promote a safe online environment.

Our submission therefore does not object to the underlying intention behind the legislation and Draft Determination, which is to provide appropriate online safety protections for the Australian community. Instead, we seek improvements in the Draft Determination to provide clarity, enable procedural fairness, and reduce regulatory complexity and burden for businesses (as well as the eSafety Commissioner) in order for them to better understand and meet their obligations.

1. Previous issues with Online Safety Bill

We note that this Draft Determination follows on from our submissions to previous consultations including by the Department and Senate Standing Committees on Environment and Communications. Throughout these consultation stages, we raised particular issues with respect to: scope of the Act in terms of extent of application, targeted businesses, types of conduct and harm; interrelated areas of reform; existing protections against cyber bullying of adults; existing industry standards and business practices relevant to the BOSE; and need for proper legislative and regulatory oversight.[1]

Despite these concerns, they remain outstanding since the passing of the legislation. We consider that there is an opportunity to clarify the Draft Determination that may – to some extent – address our previously raised concerns around the legislation.

[1] Ai Group submission to Senate Standing Committees on Environment and Communications inquiry on Online Safety Bill (Submission No. 42, 5 March 2021), https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Environment_and_Communications/OnlineSafety/Submissions; Ai Group submission to Department (12 February 2021), https://www.aigroup.com.au/news/submissions/2021/exposure-draft-of-online-safety-bill/; Ai Group submission to Department (21 February 2020), https://www.aigroup.com.au/news/submissions/2020/proposed-new-online-safety-act/.

2. Extent of targeted businesses

As noted earlier, many businesses have the capability of having an online business or platform, with online services delivered via various digital media (e.g. websites, social media, apps and other digital or online platforms) which are B2C or B2B in nature, and affect businesses of all sizes. We recommend that the scope of the Draft Determination be reviewed to ensure that it does not inadvertently and unintentionally capture a wide range of businesses than was originally intended.

Regarding potential breadth of businesses captured under the Draft Determination, these are the same issues that we raised in our submissions to the Department and Senate Standing Committees on Environment and Communications.

However, if it is the intention for the legislation to capture a wider range of businesses, it is important that the Department appreciates the diversity of businesses, and therefore provide a proportionate response and design the Draft Determination accordingly. This includes ensuring that the list of reasonable steps takes into account the diversity of many businesses (including according to their size and sectors).

We also strongly encourage appropriate support be provided to businesses that are required to meet these BOSE requirements, especially for SMEs and wider industry that may have not traditionally been subject to these types of reforms. Although we understand that the eSafety Commissioner is currently consulting on industry codes under the Online Safety Act, we consider more support be provided in the form of transition support e.g. funding from Government to uplift business capabilities to meet the requirements under the Online Safety Act including the Draft Determination. It is important to note that this is not necessarily about providing funding support for large technology businesses, but about SMEs and wider industry that may be captured under these requirements.

3. Interrelated reforms, and legislative and regulatory scope creep

In addition to the Department's consultation, there are several other reforms underway that the Department should be mindful of and avoid potential scope creep and overlap within its Draft Determination. These include:

- eSafety Commissioner's consultation on developing industry codes under the *Online Safety Act 2021* (Cth);[2]
- Parliamentary Joint Committee on Law Enforcement's inquiry into the *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019* (Cth);[3]
- Attorney General's Department's review of the *Privacy Act 1988* (Cth);[4]
- Attorney General's Department's consultation on the Exposure Draft of the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 (Cth);[5]
- Department of Home Affairs' consultation on cyber security regulations and incentives;[6]
- Department of Home Affairs' critical infrastructure security reforms;[7] and
- Treasury's consultation on an economy-wide Consumer Data Right.[8]

Related to the above, there are also existing legislations and regulations in place that the Draft Determination should avoid duplicating, as we have raised in previous submissions.

Given the potential overlap in regulatory scope including scope creep between these areas of reform, we also recommend that consideration be given to improved coordination within Government on these matters.

Without properly considering the scope, we consider that the Draft Determination could create unnecessary regulatory compliance burden and costs for a wide range of businesses that would also

[2] https://www.esafety.gov.au/about-us/consultation-cooperation/industry-codes-position-paper.
[3] https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Law_Enforcement/AVMAct.
[4] https://www.ag.gov.au/integrity/consultations/review-privacy-act-1988.
[5] https://consultations.ag.gov.au/rights-and-protections/online-privacy-bill-exposure-draft/.
[6] https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/cyber-security-regulations-incentives.
[7] https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/protecting-our-critical-infrastructure-reforms-engagement.
[8] https://treasury.gov.au/consultation/c2021-182135.

be inconsistent with the Australian Government's deregulation agenda.[9] It would also be an administratively inefficient outcome and inappropriate use of public resources if there were to be overlapping regulations and therefore overlapping responsibilities between regulators.

For instance, the following are several examples from the Draft Determination that overlap with existing legislation or regulation that should be amended accordingly:

- Section 6 relates to expectations on the provider to take reasonable steps to ensure safe use. Under this provision, section 6(3)(c) refers to reasonable steps that could include: "ensuring that persons who are engaged in providing the service, such as the provider's employees or contractors, are trained in, and are expected to implement and promote, online safety". As raised in our previous submission, section 789FD of the *Fair Work Act 2009* (Cth) covers the scenario where an employee is bullied at work and the scope of this provision extends to the use of social media while performing work at any time or location. Although the Draft Determination takes a different approach, the anti-bullying provision in the Fair Work Act might render the application of the Draft Determination unnecessary in the workplace context. The Draft Determination should also avoid eroding or restricting an employer's ability to remedy such employee conduct online. Consideration should be given to narrowing the definition to relevant persons as opposed to employees or contractors in general.

- Section 7 refers to the expectation that the provider will consult with the eSafety Commissioner and refer to their guidance in determining reasonable steps to ensure safe use. While well-intentioned, this presents a significant regulatory burden for both the Commissioner and businesses to assess the design and compliance of every single product (akin to a product compliance officer). There are potential administrative efficiencies to be gained for both the eSafety Commissioner and businesses to promote a collective approach to meeting the requirements under section 7. For example, active engagement with the Commissioner on developing industry codes through membership in industry associations under the *Online Safety Act 2021* (Cth) is an example of this occurring in practice, which could demonstrate meeting the requirements of section 7. Another example of a reasonable step could be where safety-by-design principles and assessment tools are adhered to at scale.[10] These could be included as additional examples of reasonable steps under section 7.

- Section 8 proposes an additional expectation for the provider to take reasonable steps regarding encrypted services: "If the service uses encryption, the provider of the service will take reasonable steps to develop and implement processes to detect and address material or activity on the service that is or may be unlawful or harmful". We do not consider this is an appropriate vehicle for addressing the use of encryption by service providers. Matters related to encryption are covered under the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth). Notwithstanding this, we also note that there are technical limitations posed by encryption that makes it practically difficult to implement.

- Section 9 refers to an additional expectation where the provider will take reasonable steps regarding anonymous accounts. As part of this, section 9(2)(b) considers reasonable steps could include "having processes that require verification of identity or ownership of accounts". By its definition, anonymous accounts are designed to be anonymous. This requirement also creates potential conflicts with other legislation such as the Privacy Act and Australian Consumer Law.

- Section 14 deals with the additional expectation for the provider to ensure service has terms of use, certain policies etc. Under this provision, it refers to policies and procedures with respect to the safety of end-users. Note 2 for this provision indicates that "the policies and procedures might deal with the protection, use and selling (if applicable) of end users' personal information". As this is privacy related, we do not consider it appropriate to address this matter here and it should be considered under the remit of the Privacy Act and responsibility of the OAIC.

[9] https://deregulation.pmc.gov.au/.
[10] https://www.esafety.gov.au/about-us/safety-by-design/assessment-tools.

4. Clarification of definitions and requirements

In addition to the above, the Draft Determination includes a range of other terms, definitions and requirements that would benefit from further clarification to enable targeted businesses to better understand and meet their obligations. These include:

- The term "harmful" (and its variations) is neither defined in the Online Safety Act nor the Draft Determination, which makes it subjective and vague to interpret and apply its meaning in practice. As the BOSE requirements rely on these unclear thresholds, it becomes difficult for businesses to properly understand and comply with such requirements. The definition needs to properly define "harmful", which should be limited within the scope of the Online Safety Act i.e. adult cyber abuse, image-based abuse and cyber-bullying material.

- As part of the considerations in section 6 on the service provider taking reasonable steps to ensure safe use, an additional reasonable step that should be included is where the provider implements measures *before* content is put into service.

- Section 6(3)(b) refers to the provider taking reasonable steps to ensure safe use that could be taken "if a service or a component of a service (such as an online app or game) is targeted at, or being used by, children (the children's service)—ensuring that the default privacy and safety settings of the children's service are robust and set to the most restrictive level". The term "children's service" in this provision has the potential to cover almost every service in Australia, even those not targeted or marketed for children – in other words almost any service could be used by children. A clearer interpretation could be to define children's services to be those that are specifically designed to appeal to or marketed to children. In addition, the term "most restrictive level" with respect to default privacy and safety settings of a children's service does not contemplate the scenario where there is a single level of restrictiveness, which renders the intention behind this term as inappropriate.

- Section 12 refers to a core expectation where the provider will take reasonable steps to prevent access by children to class 2 material. As part of this, section 12(2) considers reasonable steps. Reasonable measures that do not appear to have been contemplated that may be worth including in this provision are parental controls, and credit card information to access services or content.

- Section 16 refers to an additional expectation for the provider to make accessible information on how to complain to the eSafety Commissioner. However, it may not have contemplated whether this is reasonably practicable to do so such as for a global service. It may be more appropriate for the eSafety Commissioner to promote itself through relevant Government channels and advertising.

5. Safeguards and procedural fairness

The Draft Determination includes a range of obligations that would benefit from inclusion of additional safeguards for businesses such as protection of sensitive information, relevant types of complaints, and transparency in regulatory decision-making.

The following are examples of where these might arise in the Draft Determination that should be clarified:

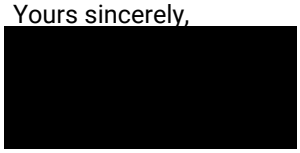
- Section 17 refers to the additional expectation where the provider will make information accessible on terms of use, policies and complaints etc. While providing transparency of online safety policies and procedures is important, there are some internal policies that may be classified as sensitive, confidential or proprietary (e.g. operational information to prevent critical systems from being abused or manipulated that could diminish online safety or security). Therefore, such information should be protected from disclosure.

- Section 20 refers to core expectations of the provider to provide requested information to the Commissioner. Information on complaints should be limited to online safety matters of a service by Australian end users.

- The Commissioner's guidance to service providers on what constitutes reasonable steps should be transparent and made publicly available. The draft declaration should include on what considerations it will take into account when assessing whether the efforts reported by a service provider under an expectation meets the "reasonable steps" test in those particular circumstances; for example: contextual information regarding the risk of harm posed by the particular service type; the relevance of the expectation to the particular service type in question; the size and maturity of the relevant service; and regulatory impact on businesses when considering what steps are reasonable.

If you would like clarification about this submission, please do not hesitate to contact me or our adviser Charles Hoang (02 9466 5462, charles.hoang@aigroup.com.au).

Yours sincerely,



Louise McGrath
Head of Industry Development and Policy