The Australian Industry Group
51 Walker Street
North Sydney NSW 2060
PO Box 289
North Sydney NSW 2059
Australia
ABN 76 369 958 788

21 February 2020

Director
Online Safety Research and Reform Section
Commonwealth Department of Infrastructure, Transport, Regional Development & Communications
Email: onlinesafety@communications.gov.au

Dear Sir/Madam

PROPOSED NEW ONLINE SAFETY ACT

The Australian Industry Group (Ai Group) welcomes the opportunity to make a submission on the Discussion Paper in relation to a new Online Safety Act proposed by the Commonwealth Department of Infrastructure, Transport, Regional Development & Communications (Department).

1. Introduction

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 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 in a diverse range of areas. In this mix, the eSafety Commissioner has an important specific role to promote a safe online environment.

As a matter of good regulatory practice, any proposed changes to existing laws and regulations, or the creation of new, should be rigorously reviewed and properly consulted on. This should include a proper analysis and assessment of issues, underlying causes, options to address these issues, as well as a robust and considered cost-benefit assessment for any proposed regulatory or legislative change. In the context of this consultation, the same level of scrutiny should be given to the Department's proposals about online safety.

At this stage, we would like to provide preliminary views. As further consultation is undertaken, there may be additional matters raised.

We would also welcome the opportunity to work closely with policy makers, governments and regulators as the review progresses.

2. Scope of proposals

It is important that the Department's proposals are clear in scope. This will enable proper assessment of the impacts of the proposals, taking into consideration existing legislation, regulations and consultations, and the range of businesses that might be captured. In the absence of properly understanding and clarifying the scope, there is a strong risk of inadequate consultation, scope creep and regulatory fragmentation, which will ultimately impact businesses – similar issues that we raised during the ACCC's Digital Platforms Inquiry. We are also mindful of the risks of unintended consequences for businesses and the community as seen with the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth).

2.1 Scope of application

The Discussion Paper suggests that the applicability of the Department's proposals is not limited to large social media companies and Australian internet service providers (ISPs), but would also apply to different types of "online service providers". Many businesses have online services delivered via various digital media (e.g. websites, social media, apps and other digital or online platforms) which are

The Australian Industry Group
51 Walker Street
North Sydney NSW 2060
Australia
ABN 76 369 958 788

B2C or B2B in nature, and affect businesses of all sizes. It is not clear in the Discussion Paper what specific businesses and services are being targeted and the extent of the impacts the Department's proposals may have.

Relevant electronic services

As an example, the Discussion Paper indicates that it would extend the cyberbullying regime, and introduce a new cyber abuse scheme for adults, applicable to all forms of social media services, "relevant electronic services" and designated internet services, and to those that host any of those services.

According to section 4 of the *Enhancing Online Safety Act 2015* (Cth):

> *"relevant electronic service" means any of the following electronic services:*
> *(a) a service that enables end-users to communicate, by means of email, with other end-users;*
> *(b) an instant messaging service that enables end-users to communicate with other end-users;*
> *(c) an SMS service that enables end-users to communicate with other end-users;*
> *(d) an MMS service that enables end-users to communicate with other end-users;*
> *(e) a chat service that enables end-users to communicate with other end-users;*
> *(f) a service that enables end-users to play online games with other end-users;*
> *(g) an electronic service specified in the legislative rules.*

There may be elements of activities of many Australian businesses that allow, for example, customer feedback and chat features with staff that may be captured by the above definition of "relevant electronic service" and therefore could fall within the scope of the Department's proposals. Additionally, there are existing tools that are offered by social media services to empower adults to report bad behaviour including against cyberbullying. In this regard, there may be adequate tools in place to protect adults against cyberbullying online, which do not necessitate the Department's proposal to extend the cyberbullying regime to adults.

Finally, cloud infrastructure providers and other similar storage or infrastructure providers may be captured, even if they have minimal or no control over the content of communications. To that end, the definition of "online service provider" should be clear and precise and should exclude services such as cloud computing.

Types of conduct and harm

In addition to the vagueness of services and businesses being targeted in the Discussion Paper, the Paper refers to many varying standards relating to harm. This creates confusion about the types of acts, omissions, standards of behaviour and conduct that are being addressed, and from whose perspective harm should be assessed. While illegal acts are capable of being recognised, some content may only harm persons of a certain disposition. There are risks that arise from uncertainty if it were to be left to the judgment of the eSafety Commissioner to make a determination as to the definition.

Ai Group recommendation:

The Department should provide greater clarification on the scope of its proposals, including definitions, with respect to:

- ***types on online services that are being targeted;***
- ***size of businesses;***
- ***nature of business interactions;***
- ***types of acts, omissions, standards of behaviour and conduct that are being addressed; and***

- ***from whose perspective harm should be assessed.***

2.2 Scope of policy issues

We note that there are interrelated issues to this consultation such as privacy and data use, cyber security and defamation. The Discussion Paper acknowledges these policy reform areas are currently under review (i.e. ACCC's Digital Platforms Inquiry and 2020 Cyber Security Strategy) and intended to be treated outside of this consultation. However, there is still a risk of overlapping issues if the scope of the consultation is not properly understood.

Further, we wish to bring to the Department's attention a relevant broader Treasury consultation currently underway which is aimed at improving the effectiveness of the consumer product safety system. Insofar as it relates to the consumer, online safety may also fall under the scope of Treasury's consultation.

Ai Group recommendation: Given the potential overlap between the separate reviews by the Department and Treasury, as well as other Government consultations, the Department should clearly outline how its online safety proposals will fit with other relevant Government consultations.

3. Existing protections against cyber bullying of adults

As a matter of course, it is important that any proposal regarding online safety avoid duplicating existing legislation or regulation that would otherwise create conflicting laws and unnecessary regulatory red tape.

For instance, with respect to the Department's proposal to establish a new cyber abuse scheme for adults, we are not opposed to the concept in principle. However, existing provisions pertaining to adults that operate in the workplace might make its proposal redundant for these particular circumstances.

Under section 789FD of the *Fair Work Act 2009* (Cth), this provision covers the scenario where an employee is bullied at work. The scope of this provision extends to the use of social media while performing work at any time or location. This was elaborated further by a Full Bench of the Fair Work Commission, which held that the reference to bullying "at work" in section 789FD was broader than when an employee is performing work in the workplace:[1]

> *[49] While a worker performing work will be 'at work' that is not an exhaustive exposition of the circumstances in which a worker may be held to be at work within the meaning of s.789FD(1)(a). For example, it was common ground at the hearing of this matter that a worker will be 'at work' while on an authorised meal break at the workplace and we agree with that proposition. But while a worker is on such a meal break he or she is not performing work. Indeed by definition they are on a break from the performance of work. It is unnecessary for us to determine whether the provisions apply in circumstances where a meal break is taken outside the workplace.*
>
> *[50] In our view an approach which equates the meaning of 'at work' to the performance of work is inapt to encompass the range of circumstances in which a worker may be said to be 'at work'.*
>
> *[51] It seems to us that the concept of being 'at work' encompasses both the performance of work (at any time or location) and when the worker is engaged in some other activity which is authorised or permitted by their employer, or in the case of a contractor their principal (such as being on a meal break or accessing social media while performing work).*

[1] *Bowker v DP World Melbourne Limited* [2014] FWCFB 9227 (19 December 2014).

…

[55] During the course of oral argument counsel for the MUA submitted that the worker would have to be 'at work' at the time the facebook posts were made. We reject this submission. The relevant behaviour is not limited to the point in time when the comments are first posted on facebook. The behaviour continues for as long as the comments remain on facebook. It follows that the worker need not be 'at work' at the time the comments are posted, it would suffice if they accessed the comments later while 'at work', subject to the comment we make at paragraph 51 above.

Although the Department's proposal takes a different approach, the anti-bullying provision in the Fair Work Act might render the application of the proposal unnecessary in the workplace context.

Similarly, decisions of the Fair Work Commission have also recognised the ability for employers to take remedial action in relation to inappropriate conduct online by employees, where there is a clear connection to the workplace (such as unlawful harassment, including sexual harassment).[2] This particularly concerns the unfair dismissal provisions in the *Fair Work Act 2009* (Cth). Employer ability to remedy such employee conduct online should not be eroded or restricted by the Department's proposal.

Ai Group recommendation: The Department should take into proper consideration other relevant legislation or regulations that might conflict with its online safety proposals e.g. Fair Work Act in relation to cyber bullying.

4. Basic online safety expectations

The Department proposes to establish a set of basic online safety expectations (BOSE) for industry, initially applying to social media companies, with the eSafety Commissioner empowered to extend its application to other specified types of online services. The Department considers this would be complementary to the eSafety Commissioner's development of voluntary safety-by-design principles and draws on the Department's Online Safety Charter. Although the BOSE is not mandatory at this stage, the Department's proposal would entail mandatory transparency reporting on how the BOSE requirements are met. The rationale for the Department's proposal is that it believes industry should be encouraged to go beyond compliance and instead actively pursue best practice with respect to online safety.

4.1 Existing industry standards and business practices

Generally, we are not opposed to a safety-by-design approach supported by principles, with the ultimate objective of protecting the safety of the Australian community. In this context, Government should reinvigorate best practice regulation initiatives, by taking into account existing business practices and study global best practices in regulation and business support that encourage – rather than inhibit – innovation and productivity.

For instance, it is not uncommon for companies to adopt internal codes of practice or conduct relating to social media use and other online activities in the workplace. It is not clear in the Discussion Paper whether consideration has been given to the effectiveness of existing internal business practices.

Further, 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. 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. This would help to reduce compliance burden for a potentially diverse range of businesses.

[2] *Ronald Anderson v Thiess* [2015] FWCFB 478 (30 January 2015); *O'Keefe v The Good Guys* [2011] FWC 5311 (11 August 2011).

The Australian Industry Group
51 Walker Street
North Sydney NSW 2060
Australia
ABN 76 369 958 788

We note the Discussion Paper's recognition of global responses to online safety. We would also like to bring to the Department's attention of international forums such as ISO/IEC that have developed relevant standards applicable to safety-by-design, which have not been mentioned in the Discussion Paper. These include:

- ISO 10000 family, including ISO 10001:2018 *Quality management – Customer satisfaction – Guidelines for codes of conduct for organizations*, and ISO 1002:2014 *Quality management – Customer satisfaction – Guidelines for complaints handling in organisations*
- ISO 20488:2018 *Online consumer reviews — Principles and requirements for their collection, moderation and publication*
- ISO 31000:2018 *Risk management – Guidelines*
- ISO/IEC 27701:2019 *Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines*
- ISO/IEC 38500:2015 *Information technology – Governance of IT for the organisation.*

4.2 Extension to other services

While we appreciate the intention to give the eSafety Commissioner flexibility, we do not consider it appropriate simply to empower the eSafety Commissioner to extend the BOSE to other types of services. There should be rigorous scrutiny of any expansion of the scope of the BOSE. There should be transparency, a requirement for genuine consultation and consideration of regulatory impacts and clear oversight and accountability in relation to any changes. The most straightforward way to achieve this would be to require a clearer definition of the scope of the proposed legislation and a requirement for legislative change to expand its scope.

Ai Group recommendation:

If the Department were to consider pursuing a set of basic online safety expectations for industry, it should take into consideration:

- ***Effectiveness of existing internal business practices that address online safety;***
- ***Flexibility to accommodate regulatory changes within individual business practices;***
- ***Global best practice approaches including international standards and whether they are suitable in the Australian context;***
- ***A suitable forum such as Standards Australia to consider international standards discussions that impact on a wide range of sectors; and***
- ***Extending the BOSE to other specified types of services should be subject to sufficient regulatory accountability and oversight (e.g. through legislative change).***

5. Uncertainty on proposed default privacy settings

The Department proposes in its Discussion Paper for online service providers that make products marketed to children to be required to default to the most restrictive privacy and safety settings at initial use or set-up of the product. However, section 2.1 of the Online Safety Charter, which will inform the proposed BOSE, takes a further significant step and sets an expectation 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".[3] That is, the Charter's consideration of default privacy settings is much more broader in application than the Department's proposal, and will likely have wider implications for businesses and consumers.

And although the proposed BOSE is not mandatory at this stage, the Government has stated in the Charter that it "will take into account the extent to which technology firms and digital platforms operating in Australia are meeting the expectations set out in the Charter when assessing the need for further regulatory reform".[4]

[3] Australian Government, Online Safety Charter, December 2019, p. 4.
[4] Australian Government, Online Safety Charter, December 2019, p. iii.

The Australian Industry Group
51 Walker Street
North Sydney NSW 2060
Australia
ABN 76 369 958 788

As a consequence, the Discussion Paper does not address the potential regulatory and consumer impact of requiring broader online services (i.e. those not marketed to children) to default to the most restrictive privacy and safety settings. For example, consideration will need to be given on user experiences of many common digital platforms and services, and business impacts on organisations providing those services.

Ai Group recommendation: The Department should clarify the scope of the proposed baseline online safety expectations concerning privacy and safety defaults for services that are not marketed to children.

6. Shortening take-down notice time

The Department proposes to shorten the take-down time for cyberbullying and image-based abuse schemes for online service providers from 48 to 24 hours.

While this timeframe may already be achieved by some online service providers on a voluntary basis, as suggested in the Discussion Paper, it may not necessarily be the same for others. And if the definition of online service providers were to be interpreted broadly, this will likely present significant difficulty for: businesses not currently subject to these requirements who would experience a greater burden to meet these more onerous timeframes; and businesses that are based offshore, which require notices being legally served in their relevant jurisdictions.

If the Department were to consider broadening the application of the take-down notice time for cyberbullying and image-based abuse scheme to a broad range of businesses, a more appropriate timeframe should be considered. For example, alternative to specifying a timeframe, consideration should be given to "expeditious removal" with supporting guidelines that could provide examples of what this means.

Further, the proposed expanded scope of these notices should be made clear that it does not apply to providers that have minimal or no control over the content of offending material such as the underlying network or other infrastructure providers.

Ai Group recommendation:

If the Department considers broadening the scope of the cyberbullying scheme, it should:

- ***Explore an alternative timeframe for a take-down notice such as "expeditious removal" with supporting guidelines that could provide examples of what this means.***
- ***Exclude from a take-down notice providers that have minimal or no control over the content of the offending material.***

7. Additional tools to address cyberbullying

The Department proposes additional tools to address cyberbullying by providing the eSafety Commissioner with the power to compel service providers to enforce their terms of service in relation to a user who has been found to have posted cyber abuse material, apply account restrictions in serious cases, or to request or require certain other enforcement actions.

We are deeply concerned that use of such a power may result in enforcement that, if not applied appropriately, is inconsistent with service providers' global approaches and is a direct form of Government intervention that encroaches upon the sanctity of private contracts. This also raises the importance of accountability and transparency in the regulatory process.

Alternative measures should be explored further in consultation with industry.

The Australian Industry Group
51 Walker Street
North Sydney NSW 2060
Australia
ABN 76 369 958 788

Ai Group recommendation: The Department should explore further alternative mechanisms to address cyberbullying in consultation with industry.

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

Yours sincerely,

Peter Burn
Head of Influence and Policy