The Australian Industry Group
Level 2, 441 St Kilda Road
Melbourne VIC 3004
PO Box 7622
Melbourne VIC 3004
Australia
ABN 76 369 958 788

5 March 2021

Committee Secretary
Senate Standing Committees on Environment and Communications
Email: ec.sen@aph.gov.au

Dear Committee Secretary

ONLINE SAFETY BILL

The Australian Industry Group (Ai Group) would like to make a submission on the Online Safety Bill (Bill) currently under review by the Environment and Communications Legislation Committee of the Senate Standing Committees on Environment and Communications.

Ai Group recently made a submission to the Department of Infrastructure, Transport, Regional Development and Communications (Department) on its consultation of the Exposure Draft of the Online Safety Bill.

We understand that this has now been tabled into Parliament as a Bill and referred to the Senate Standing Committees on Environment and Communications, with a very short timeframe for submissions that closed on 2 March 2021.

In our submission on the Exposure Draft Bill, we noted that we were not confident that our concerns have been properly taken into consideration at the previous consultation stage.

Given the accelerated schedule that this Bill has now proceeded to Parliament and Senate Standing Committee for review, we wish to reiterate key issues that were raised in our recent submission. For your consideration, a copy of our recent public submission to the Department that outlines our key issues is enclosed to this cover letter for your reference.

If you would like clarification about this submission, please do not hesitate to contact me

Yours sincerely,

Louise McGrath
Head of Industry Development and Policy

The Australian Industry Group
Level 2, 441 St Kilda Road
Melbourne VIC 3004
PO Box 7622
Melbourne VIC 3004
Australia
ABN 76 369 958 788

12 February 2021

Online Safety Branch, Content Division
Department of Infrastructure, Transport, Regional Development and Communications
Email: OnlineSafety@infrastructure.gov.au

Dear Sir/Madam

EXPOSURE DRAFT OF ONLINE SAFETY BILL

The Australian Industry Group (Ai Group) welcomes the opportunity to make a submission on the Exposure Draft of the Online Safety Bill (Draft Bill) under consultation 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.

We note that this consultation follows from the Department's Discussion Paper on a new Online Safety Act in February last year. According to the consultation page, we understand the Draft Bill has been developed following substantial public and stakeholder consultation. However, we are not confident that our concerns have been properly taken into consideration in the Draft Bill. We therefore wish to reiterate key issues that were raised in our previous submission and, to provide greater clarity and transparency, welcome feedback from the Department on how it has addressed our specific issues.

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.

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

2. Scope

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 Extent of application

The Department's previous Discussion Paper suggested that the applicability of the Department's proposals was 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 B2C or B2B in nature, and affect businesses of all sizes. In the Department's latest iteration of the Draft Bill, it is still not clear what specific businesses and services are being targeted and the extent of the impacts the Department's proposals may have.

2.1.1 Targeted businesses

As an example, the Draft Bill includes reference to a range of services including "social media services, relevant electronic services and designated internet services". The Draft Bill also refers to a range of additional services that would be subject to the new legislative requirements (in part or full) including those defined as "online activity" and "section of the online industry" (sections 134 and 135 of the Draft Bill), covering providers of the abovementioned services as well as for internet search engine services, app distribution services, hosting services, internet carriage services, and manufacturers, suppliers, maintenance and installation of equipment for such services to end users in Australia. These capture a wide range of businesses.

Focusing on "relevant electronic services", section 5 of the Draft Bill (which appears to be based on section 4 of the *Enhancing Online Safety Act 2015* (Cth)) defines this term as:

> *"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 definitions should be clear and precise and should exclude services such as cloud computing.

2.1.2 Types of conduct and harm

In addition to the vagueness of services and businesses being targeted in the Draft Bill, it explicitly refers to different forms of harm including: "serious harm" and "significant harm". While "significant harm" appears to be undefined, "serious harm" is defined under section 5 of the Draft Bill as "serious physical harm or serious harm to a person's mental health, whether temporary or permanent". And "serious harm to a person's mental health includes: (a) serious psychological harm; and (b) serious distress".

"Serious harm" is applied in section 7 of the Draft Bill relating to cyber-abuse material targeted at an Australian adult, namely: "an ordinary reasonable person would conclude that it is likely that the material was intended to have an effect of causing serious harm to a particular Australian adult".

"Significant harm" is applied in the context of blocking requests (section 95 of the Draft Bill) and blocking notices (section 99), and expressed along the following lines: "the Commissioner is satisfied that the availability of the material online is likely to cause significant harm to the Australian community".

While it appears that some attempt has been made to define the targeted individual or group that may be subject to the harm, there are still questions relating to whether these definitions are sufficiently clear to properly understand 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 of 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 Related policy issues

We note that there are interrelated issues to this consultation such as privacy and data use, cyber security and defamation. While the Department's previous Discussion Paper acknowledged these policy reform areas are currently under review and intended to be treated outside of this consultation, there is still a risk of overlapping issues if the scope of the consultation is not properly understood.

Below is a non-exhaustive list of various government consultations and initiatives that are relevant for consideration in relation to this latest consultation. Where possible, we have also referenced our previous submissions covering similar issues that may be relevant to the questions raised in this Draft Bill:

- ACCC *Digital Platforms Inquiry* – Government's response to this Inquiry includes policy reforms in the area of privacy and data regulation.[1] Following this Inquiry, the Attorney General's Department has now commenced its *Review of the Privacy Act*.[2]

- Home Affairs *Voluntary Code of Practice: Securing the Internet of Things for Consumers* – a range of matters with respect to the proposed Code of Practice that may be relevant to this consultation.[3]
- Home Affairs consultation on *Protecting Critical Infrastructure and Systems of National Significance* – we raised several issues including details that currently remain unclear and require further consultation such as the nature of the reforms, scope, definitions, measures and cost-benefit impact.[4]

- Home Affairs consultation on its draft *Critical Technology Supply Chain Principles* – a range of matters including principles that may be relevant to this consultation.[5]

[1] Ai Group submission to Treasury (September 2019), Link: https://cdn.aigroup.com.au/Submissions/Technology/AiGroup_submission_Digital_Platforms_Inquiry.pdf.
[2] Ai Group submission to Attorney-General (November 2020), Link: https://cdn.aigroup.com.au/Submissions/General/2020/Privacy_Act_Review_November_2020.pdf.
[3] Ai Group submission to Home Affairs (February 2020), Link: https://cdn.aigroup.com.au/Submissions/Technology/Securing_IoT_for_Consumers_Voluntary_Code_of_Practice_Feb_2020.pdf.
[4] Ai Group submission to Home Affairs (November 2020), Link: https://cdn.aigroup.com.au/Submissions/Technology/Home_Affairs_Critical_Infrastructure_Security_Reforms_Exposure_Draft_Bill_Nov2020.pdf.
[5] Ai Group submission to Home Affairs (November 2020), Link: https://cdn.aigroup.com.au/Submissions/Technology/Home_Affairs_Critical_Technology_Supply_Chain_Principles_Discussion_Paper_12Nov.pdf.

- Treasury consultation on *Major reforms to the Foreign Investment Review Framework* – we consider that there are potential interactions between Home Affairs' critical infrastructure security reforms and Treasury's reforms.[6]

- Treasury consultation on its *Inquiry into Future Directions for the Consumer Data Right* – we raised several interrelated issues including on privacy, data protection and cyber security.[7]

- Treasury consultation on *Improving the Effectiveness of the Consumer Product Safety System* – online safety considerations may also fall under the scope of Treasury's consultation if it leads to consumer safety issues.[8]

- Parliamentary Joint Committee on Intelligence and Security (PJCIS) and Independent National Security Legislation Monitor (INSLM) reviews relating to the *Telecommunications and other Legislation Amendment (Assistance & Access) Act 2018* (Cth) (TOLA Act) – there are concerns about the potential negative impact of this Act on cyber security and privacy of products and services.[9] We have made a supplementary submission supporting the INSLM's recommendations.[10]

- PJCIS review into the effectiveness of the *Telecommunications Legislation Amendment (International Production Orders) Bill 2020* – we consider this review is interrelated with the TOLA Act review.[11]

- Standing Committee on Communications and the Arts *Inquiry into 5G in Australia* – while cyber security has been excluded from this Inquiry, there are interrelated considerations with respect to the operation of 5G and IoT.[12]

- Ambassador for Cyber Affairs and Critical Technology within DFAT has been consulting on *Australia's International Cyber and Critical Technology Engagement Strategy*, which will potentially be relevant to this consultation.[13]

---

[6] Ai Group submission to Treasury (September 2020), Link: https://cdn.aigroup.com.au/Submissions/Trade_and_Export/Submission_FATA_reforms_September_2020.pdf .

[7] Ai Group submission to Treasury (June 2020), Link: https://cdn.aigroup.com.au/Submissions/Technology/Treasury_CDR_Inquiry_5Jun_2020.pdf.

[8] Treasury, Improving the Effectiveness of the Consumer Product Safety System, Link: https://consult.treasury.gov.au/market-and-competition-policy-division-internal/main-consultation.

[9] Joint submission to PJCIS (Submission No. 23, July 2019), Link: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/AmendmentsTOLAAct2018/Submissions; Joint submission to INSLM (Submission No. 15, September 2019), Link: https://www.inslm.gov.au/submissions/tola; Ai Group submission to INSLM (Submission No. 12, September 2019), Link: https://www.inslm.gov.au/submissions/tola; Australian Strategic Policy Institute, Perceptions survey: Industry views on the economic implications of the Assistance and Access Bill 2018 (December 2018), p. 3.

[10] Ai Group supplementary submission to PJCIS (Submission No. 23.1, July 2020), Link: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/AmendmentsTOLAAct2018/Submissions.

[11] Ai Group submission to PJCIS (Submission No. 32, May 2020), Link: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/IPOBill2020/Submissions.

[12] Ai Group submission to Standing Committee on Communications and the Arts (Submission No. 356, November 2019), Link: https://www.aph.gov.au/Parliamentary_Business/Committees/House/Communications/5G/Submissions.

[13] DFAT, International Cyber and Critical Technology Engagement Strategy, Link: https://www.dfat.gov.au/international-relations/themes/cyber-affairs/public-consultation-international-cyber-and-critical-technology-engagement-strategy.

- Australian Human Rights Commission's (AHRC) consultation into *Human Rights and Technology* – as the title suggests, the AHRC have been exploring the impact of emerging technologies on human rights.[14]

- With respect to standards, there already exists standards (especially international such as ISO/IEC) and initiatives to support industry standards relevant to AI and other related standards (such as on privacy and cyber security) that may be relevant to this consultation. These are discussed further below.

Ai Group recommendation: Given the potential overlap between the Department's consultation and 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.

3.1 Fair Work Act 2009 (Cth)

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:[15]

> *[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).*
>
> *…*
>
> *[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*

[14] Ai Group submission to AHRC (March 2020), Link: https://cdn.aigroup.com.au/Submissions/Technology/AHRC_Human_Rights_and_Technology_Discussion_Paper_26Mar_2020.pdf.
[15] *Bowker v DP World Melbourne Limited* [2014] FWCFB 9227 (19 December 2014).

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).[16] 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.

3.2 Other existing legislations and regulations

In addition to the Fair Work Act, there are other existing legislation that may also be duplicated by the Draft Bill. These include: defamation and anti-discrimination related legislations; *Enhancing Online Safety Act 2015* (Cth); *Enhancing Online Safety (Non-consensual Sharing of Intimate Images) Act 2018* (Cth); and the existing prohibition in the *Criminal Code Act 1995* (Cth) about using a carriage service to menace, harass or cause offence (section 474.14). Proper consideration of these existing legislations and regulations should be reviewed, including clarifying the scope of the Draft Bill to understand how it would interact with these other existing legislative requirements and ensure that it does not create a conflict with existing legislative and regulatory obligations.

Ai Group recommendation: The Department should take into proper consideration other relevant legislation or regulations that might conflict with its online safety proposals in relation to cyber bullying e.g. Fair Work Act, Enhancing Online Safety Act, Enhancing Online Safety (Non-consensual Sharing of Intimate Images) Act, Criminal Code Act, and defamation and anti-discrimination related legislations.

4. Basic online safety expectations

The Draft Bill proposes for basic online safety expectations (BOSE) to apply to social media services, relevant electronic services and designated internet services. The eSafety Commissioner would also be empowered to mandate providers of these services to report to it about their compliance with the BOSE, with attached penalties for failure to report.

Associated with the BOSE and setting expectations for industry, the Draft Bill also provides for the establishment of industry codes and industry standards. The eSafety Commissioner would also be empowered to request an industry code or determine an industry standard in consultation with the public, and also make a service provider determination to determine service provider rules. These codes and standards could be used by the Commissioner to assess complaints and apply various remedial actions against the service provider for non-compliance.

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 Draft Bill whether consideration has been given to the effectiveness of existing internal business practices.

Further, given the possible broad application of the BOSE reporting requirements, 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

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

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.

We note the Department's previous recognition of global responses to online safety in its previous Discussion Paper, but it is not clear whether this will be recognised in the Draft Bill. We would 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 referred to in the Draft Bill. 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 Legislative and regulatory oversight

In the previous Discussion Paper, the BOSE was proposed to initially apply to social media companies, and stated that the eSafety Commissioner would be empowered to extend the application of the BOSE to other specified types of online services. The scope of the BOSE in the Draft Bill appears to now not be limited to social media services at the outset, and could also apply to relevant electronic services and designated internet services.

Our previous concern related to the need for 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.

With respect to the latest iteration of the Draft Bill, we consider that regulatory oversight and accountability concerns remain. We welcome the inclusion of a public consultation process which should provide for greater transparency. Nevertheless, we recommend additional considerations be factored into the determination process to ensure better accountability and oversight, and proper weight given to relevant industry feedback.

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;***
- ***Applying the BOSE to specified types of services; and***
- ***New powers created for the relevant Minister and eSafety Commissioner should be subject to sufficient regulatory accountability and oversight (e.g. through legislative change).***

5. Shortening take-down notice time

The Draft Bill proposes to shorten the take-down time for cyberbullying and image-based abuse schemes for service providers from 48 to 24 hours. Accompanying this provision of 24 hours, the Draft Bill also provides for an alternative undefined timeframe i.e. "such longer period as the Commissioner allows".

While the proposed 24-hour timeframe may already be achieved by some service providers on a voluntary basis, as suggested in the previous Discussion Paper, it may not necessarily be the same for others. And if the definition of service providers subject to this Draft Bill 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.***

Yours sincerely,

Louise McGrath
Head of Industry Development and Policy