COMMUNICATIONS
ALLIANCE LTD

Communications Alliance

Submission

to the

Department of Infrastructure, Transport, Regional Development and Communications

Exposure Draft
Online Safety Bill 2020

12 February 2021

CONTENTS

1. ABOUT COMMUNICATIONS ALLIANCE

Communications Alliance is the primary telecommunications industry body in Australia. Its membership is drawn from a wide cross-section of the communications industry, including carriers, carriage and internet service providers, content providers, equipment vendors, IT companies, consultants and business groups.

Its vision is to provide a unified voice for the telecommunications industry and to lead it into the next generation of converging networks, technologies and services. The prime mission of Communications Alliance is to promote the growth of the Australian communications industry and the protection of consumer interests by fostering the highest standards of business ethics and behaviour through industry self-governance. For more details about Communications Alliance, see http://www.commsalliance.com.au.

In March 2014, Communications Alliance assumed responsibility for the industry codes and core responsibilities of the Internet Industry Association (IIA) (which was in the process of dissolving). Consequently, Communications Alliance became the owner of the IIA industry codes, including the *Hosting Content Within Australia Code*, the *Providing Access To Content Hosted Within Australia Code* (together the Internet and Mobile Content Codes) and the *Content Services Code*. Communications Alliance also took over responsibility for the Family Friendly Internet Filter scheme (FFF) scheme (including the Ladybird Logo).

2. INTRODUCTION

Communications Alliance welcomes the opportunity to make a submission in response to the Exposure Draft of the *Online Safety Bill 2020* (Exposure Draft) released for public consultation by the Department of Infrastructure, Transport, Regional Development and Communications, (Department) on 23 December 2020.

We agree with the general premise that a revised approach to some of the underlying legislative framework is timely – if not overdue – to ensure that the online world is governed by technology and platform-neutral, practical and principles-based rules that, to the greatest extent possible, are able to flexibly adjust to the dynamic environment to which they pertain.

The lives of Australians and the citizens of most nations worldwide, are increasingly influenced by an online environment in which they participate actively or passively. Access to the internet is almost universal in most developed countries and is, in those countries, increasingly considered to be a human right or at least a catalyst for human rights. The internet has become not only an essential tool for formal and informal education in all areas of society, but is also a key mechanism for communication, engagement and leisure activity. With one of the highest smart-phone penetration rates in the world and fast and reliable mobile internet in most of the populated areas of Australia, this online environment is now almost always available at our fingertips.

Australian governments have created rules, guidelines and behavioural expectations on how to keep individuals safe in our physical environments (e.g. on our roads, in maritime situations, national parks, etc.) while allowing them to enjoy these physical environments and ensuring that the ecosystem of this environment can remain intact. In much the same way, our society must create and apply certain standards for our online environment to ensure the safety of its citizens and provide the conditions in which the online world can continue to evolve and furnish the services that we have come to love and depend on. A safe online environment is a shared responsibility of Government, Industry and end-users.

The communications industry recognises that access to some online content, particularly by minors or vulnerable adults, may have detrimental effects on the physical, social and emotional well-being of the user, and that access to some content by some user groups may also influence their values with regards to sexuality, relationships, violence, security, racial and religious equality, tolerance and many other key societal values. The proliferation of online social networking poses additional challenges around cyber-abuse and the unwanted sharing of (sometimes intimate) images. In this context, it must be noted that social media platforms and search engines dedicate vast amounts of time and resources to minimise abuse of their services and potential harm that may result from content that is accessible through their services. The overwhelming majority of abuses are detected and removed by the major platforms proactively and without requiring or using an internal or external escalation mechanism.

It goes without saying that illegal content, especially material relating to child sexual abuse and terrorism, must be eradicated to the extent possible and as quickly as possible, to minimise the detrimental effects on all parties involved.

As in the past, our industry continues to engage closely with all stakeholders, including enforcement agencies, and is keen to assist, where possible, to create, maintain and promote a safe online environment.

3. COMMENTS AND OBSERVATIONS

3.1. Interaction of the Act with other pieces of legislation/regulation

We understand that the proposed Online Safety Act is intended to replace the *Enhancing Online Safety Act 2015*. As already highlighted in our submission to the Reviews of the *Enhancing Online safety Act 2015* and the Online Content Scheme (OCS) in July 2018 as well as our submission to the Online Safety Legislation Reform Discussion Paper in 2020, we welcome an approach that seeks to consolidate the various pieces of legislation and regulation that currently form the online safety framework, including Schedules 5 and 7 of the *Broadcasting Services Act 1992* (BSA), into a single piece of legislation.

Against this background we note that it is not clear whether and, if so, in what manner and through what processes other pieces of legislation and regulation, including the relevant Schedules of the BSA and the *Restricted Access Systems Declaration 2014*, will be amended to ensure a coherent and consolidated online safety framework.

The prescriptiveness of the current Schedules 5 and 7 of the BSA has so far prevented a meaningful review of the existing content-related codes and will continue to do so if the Schedules are not substantially revised. This is especially relevant, given Parliament's intention that one or more industry codes (or standard(s)) be registered within 6 months (or 12 months for a standard) after the commencement of Part 9, Division 7, of the proposed Act. We provide further commentary on the timeframe for the registration of industry codes in Section 3.3 of our submission.

In this context it is also worth noting that the review of the classification regulation has not concluded and, accordingly, it is not clear how potential findings of this review will interact with the proposed new Online Safety Act, especially with Part 9, Online Content Scheme, of the draft legislation.

Similarly, Stage 1 of the NSW-led review of the defamation law in Australia (Model Defamations Provisions) has not yet been enacted in State and Territory legislation and, importantly, Stage 2 of the reform process, focusing on the responsibilities and liability of digital platforms for defamatory content published online, is yet to commence. This is relevant as we see a potential overlap of defamation-related content and the proposed adult cyber-abuse scheme of the Exposure Draft.

3.2. Basic Online Safety Expectations

Part 4, Section 45, allows the Minister to determine, by legislative instrument, basic online safety expectations (BOSE) for social media services, relevant electronic services and designated internet services.

It is unclear whether it is intended that the Minister determines such BOSE at the same time as the new Online Safety Act comes into force, or at a later stage. If the Minister indeed intends to determine BOSE – which must contain minimum expectations in accordance with Section 46 of the draft legislation – then it would be beneficial for Industry to receive such expectations as early as possible in order to avoid duplication and additional complications (e.g. with respect to the development of processes to ensure compliance and internal and reporting documentation) when implementing other requirements of the new Act.

Industry would also welcome consultation prior to the BOSE being determined.

We also highlight that compliance with any additional reporting obligations will necessarily increase costs for industry. Consequently, careful consideration ought to be given to the scope of such reporting obligations to ensure that the benefits of such obligations outweigh any attendant costs.

3.3. Development of industry codes

Part 9, Division 7, outlines Parliament's intention that industry codes and/or standards be registered by the eSafety Commissioner within 6 months (for codes) and 12 months (for standards) of the commencement of Division 7.

We welcome the inclusion of provisions for co-regulatory industry codes to be registered by the eSafety Commissioner who we believe will be best qualified to deal with industry codes on the envisaged subject matters.

A co-regulatory approach will help to ensure that a future online safety framework is sufficiently flexible to promptly accommodate future technological and societal changes that will undoubtedly – and most likely at an even faster pace – occur in this area. The deployment of 5G, the burgeoning influence of the Internet of Things, progress in relation to virtual and augmented reality and the creation and widespread use of artificial intelligence serve as examples of significant technological change already influencing our online lives.

Over the past two decades, Communications Alliance has developed and revised hundreds of industry codes and standards for various elements of the communications industry and the related consumer experience environment. Drawing on this experience, we are concerned that the proposed timeframe of 6 months for registration (as opposed to development of a draft for consideration for registration) of an industry code, is extremely short or indeed unrealistic. This timeframe becomes even more unrealistic considering that several codes are likely to be required to cater for the needs of the different sections of the online industry.

Our current code development and registration process (with the Australian Communications and Media Authority) typically entails the following steps:

1. Call for industry working committee members to ensure the relevant industry participants have an opportunity to contribute to the process, ensuring adequate and proportionate representation;
2. Definition of the terms of reference;
3. Development of a draft code;
4. Liaison with the ACMA (and other relevant stakeholders such as the Australian Communications Consumer Action Network (ACCAN), Australian Competition and Consumer Commission (ACCC), Office of the Australian Information Commissioner (OAIC), DITRDC etc.) over the draft code throughout the drafting process;
5. Opportunity for the ACMA Authority to consider a pre-public comment version of the code;
6. Refinement of the draft code, incorporation of ACMA (or other stakeholder) feedback;
7. Public comment period (minimum of 30 days) and formal consultation with key stakeholders;
8. Due consideration and incorporation of public comment feedback by the working committee;
9. If the public comment draft has been altered in a material way as a result of the public comment, a second public comment period (again a minimum of 30 days) plus subsequent consideration/incorporation of additional feedback;
10. Obtaining mandatory certificates of consultation from key stakeholders (not required as per the Exposure Draft);
11. Compilation of the relevant registration documentation, including documentation that Communications Alliance has duly discharged of all consultation and feedback consideration requirements;
12. Submission for registration

13. Consideration by the ACMA Authority and, if agreeable, approval for registration;
14. ACMA processes to place the code on the Register of Legislation;
15. Gazetting of code, thereby giving effect to the code.

While codes under Division 7 of the proposed legislation are to be registered with the eSafety Commissioner – who may also need to familiarise herself with the new powers and processes involved – instead of the ACMA, we believe that the above demonstrates that it is unrealistic or impossible to achieve registration of a new industry code, let alone a multitude of codes (which typically require the same resources within service providers) within an allocated timeframe of 6 months.

We also note that the registration of an industry standard, which can be drafted by a single party (i.e. the eSafety Commissioner) without the pre-public comment involvement of various industry participants, is proposed to be afforded twice as much time, i.e. 12 months.

As noted above, we commend the inclusion of the intention for industry to develop codes for relevant sections of the online industry. Section 145 of the Exposure Draft empowers the Commissioner, possibly by direction of the Minister, to determine an industry standard without allowing industry to first attempt a code. However, in the interest of fostering genuine industry-Government collaboration and enabling the design of regulations that are practical and cater to the needs of each industry section, the draft legislation ought to require the Commissioner to give the relevant industry association at least 6 months to first develop a draft industry code before the Commissioner can move to create a standard and only if the draft code demonstrably does not meet community safeguards.

It is also worth highlighting that our industry has consistently urged Government to review Schedules 5 and 7 of the BSA (and other online safety legislation for that matter) and we have been told since 2015 that a Discussion Paper, initiating the review process, was imminent. It is therefore difficult to understand why the proposed legislation includes unrealistically tight timeframes – or indeed timeframes at all (see below) – for code registration. Importantly, the current prescriptiveness of Schedules 5 and 7 of the BSA would prevent the development of meaningful codes, i.e. it is not possible to even commence a code development process prior to having an understanding of the content/construct of the new Schedules 5 and 7 of the BSA. We also reiterate our concern that this legislative process interacts with the defamation law review process and potentially also the review of the *Privacy Act 1988,* both of which may impact on a code development process.

Generally, it appears that it might be worth to get a better understanding of the 'gaps' that may still exist once the Act has been implemented and only then complement the legislation with industry codes.

Consequently, we request that the timeframe for registration of industry codes under Division 7 of the Exposure Draft be removed from the Act. Instead, we propose that the subordinate legislative instrument requesting the development of an industry code stipulate the timeframe for registration and that this timeframe be no less than 12 months. Stipulating the timeframe for registration in a subordinate legislative instrument would be in in line with approach taken by Part 6 of the *Telecommunications Act 1997* which does not (and never has, also not in its original version in 1997) prescribe a timeframe for registration of industry codes (or standards for that matter) from enactment.

3.4. Behavioural change and end-user notices

We welcome the release of the Exposure Draft and, in principle, align behind many of the proposed measures. It is important to ensure that young and vulnerable Australians, in particular, can safely enjoy the benefits that the internet brings for our society.

However, we caution against the notion that a new legislated online safety framework will be sufficient to bring about significant change. In order to achieve the latter, it will be key to

continue and to enhance educational measures, including through Government-led online safety campaigns which focus on end-user responsibilities.

To this end we have already developed a set of messages – in cooperation with the Commissioner – which we have made available to Government for inclusion into a Government-funded educational campaign. Such a campaign ought to be similar to previous efforts to raise awareness about the dangers of sun burns and the effectiveness of applying sunscreen (Slip, Slop, Slap). We stand ready to continue our dialogue with all stakeholders on meaningful ways to educate end-users on how to protect themselves from potentially harmful material online.

Against this background, we urge the eSafety Commissioner to make use of her (already existing) powers to issue notices for removal of content to end-users – especially in relation to cyber-abuse material targeted at an adult – instead of confining notice requests to service providers. It is regrettable that the eSafety Commissioner, so far, has not issued such notices. We believe that the effect of issuing such notices with reasonable rigour and frequency could have similar effects on the mindset of end-users as frequent and 'notorious' speed camera/red-light checks (with associated fines) have on speeding motorists.

3.5. Scope of services

The scope of services to which the various content removal obligations apply is extensive. While the broadening of the scope of services may, prima facie, be appealing, it is not clear how the scheme would deal with some of the services now in scope in practice. For example, messaging services (e.g. WhatsApp, Signal, Telegram) are often end-to-end encrypted and may not offer an option for removal of individual parts of a conversation. Does this mean that user accounts would be required to be suspended, restricted or terminated when a complaint (that has been found valid) about cyber-abuse material has been received? It is not clear that wholesale suspension from a messaging service is a proportionate response to a report of bullying and harassment – especially given how nuanced and complex private conversations between adults can be.

Internet Service Providers (ISPs) reiterate their concern that it is neither technically feasible nor appropriate for ISPs to remove content. Therefore, where ISPs are concerned, we largely base our feedback on the Exposure Draft on the understanding that ISPs will not be required to remove content (as opposed to block access to websites that host certain material).

Against this background but also with view to potential implications with regard to the privacy of individuals, the question arises as to how the authors of the draft legislation envisage that the removal of material from SMS/MMS communications would be facilitated? We believe it is not appropriate – and in our view also not permissible under current legislation – for service providers to review and identify messaging content at a granular level.

In this context, it is also important to highlight that the consequences, i.e. the degree of harm that is likely to be incurred, are likely to be very different for content that is shared in a private messaging stream compared to the sharing of such content through public platforms accessible by a large number of individuals. In addition, private messaging services typically offer far greater controls and restrictions that enable the user to protect themselves from such harm.

Importantly, how would the eSafety Commissioner determine, in the context of a private communication between two individuals, whether a certain behaviour constitutes cyber abuse, without extensive knowledge of the context and background of that communication? This is particularly true for material that is deemed 'offensive' (refer to our discussion in Section 3.7 below), but it would also be useful to consider to what extent harassment and menacing behaviours are already prohibited through existing statute.

It is worth noting that the German *Netzwerkdurchsetzungsgesetz* (NetzDG)[Network Enforcement Act] has refrained from including private messaging services in its scope.

Equally concerning is the proposed broadening of scope to include 'designated internet services' which basically includes any website.[1] Hosting services are now also included in the scope of services covered under the draft legislation.

Many websites allow users to comment, post, chat or otherwise upload content. This includes product/service review websites, websites of clubs, schools, churches, social and charitable institutions etc. Sometimes, those content-creation/upload functions require registration or the creation of a user account. At other times these functions allow users to remain largely anonymous. Importantly, many of those websites are operated and maintained through very limited resources and/or volunteers. It appears unrealistic to expect the providers of such websites (or their hosts) to take-down content upon request within a 24-hour timeframe. We believe that many of these websites would struggle to comply, even with far longer timeframes. Please refer to Section 3.6 for further considerations on the 24-hour removal timeframe.

We note the discretion that is afforded to the eSafety Commissioner to stipulate longer removal timeframes. However, we maintain that while it may be appealing to cast the net as widely as possible from a uniformity and enforcement perspective, the proposed approach is not practical and that a case for the inclusion of all kinds of services has not been made. The discussion so far has failed to demonstrate that harm is generated by or from such websites at a level that would warrant the proposed measures.

Similarly, we believe that it is not a proportionate measure to include business-to-business services into the scope of the proposed legislation. These services typically pose very limited risk and/or have a significantly reduced capacity to address harms (as they may not be able to delete content at a granular level) and should, consequently, be excluded from the scope from the outset.

In this context, it is worth noting that the Full Government Response to the Consultation on the UK Online Harms White Paper excludes business-to-business services and other "low-risk services; for example, reviews and comments by users on a company's website which relate directly to the company, its products and services, or any of the content it publishes"[2].

The proposed cyber abuse regimes (targeted at children and adults) both include online games, game streaming and game chat services in the scope of services that are to be captured by those schemes. Many games indeed provide an internal chat function. However, without further evidence of the magnitude of the problem and, hence, any indication whether the proposed measures are proportionate, we are sceptical about the inclusion of those services. Similar problems as discussed above in the context of messaging services apply.

3.6. 24-hour removal/blocking timeframes

The Exposure Draft proposes that service providers are to remove content subject to a removal/remedial notice within 24 hours (unless specified otherwise). ISPs are to block content within 24 hours of a blocking request.

With respect to removal notices, it is unclear why a reduced timeframe for compliance with take-down requests is required. The Discussion Paper released in December 2019 correctly noted that the existing regime is operating successfully and that requests to take down material have been met promptly (at times within 30 minutes) and with a 100 percent

[1] Section 14, Designated internet service, *Online Safety Bill 2020*, Exposure Draft: "(1) For the purposes of this Act, *designated internet service* means: (a) a service that allows end-users to access material using an internet carriage service; or (b) a service that delivers material to persons having equipment appropriate for receiving that material, where the delivery of the service is by means of an internet carriage service; […]"

[2] Part 1, Services in Scope, as accessed at https://www.gov.uk/government/consultations/online-harms-white-paper/outcome/online-harms-white-paper-full-government-response on 12.02.2021

success rate. It appears unwarranted to shorten the timeframes and, at the same time, to expand the scope of services and providers captured under the scheme to include a wide variety of (often very small) services (refer to our points in Section 3.5 above). Should Government proceed with a reduction to a 24-hour time period, we believe there should be exceptions where an investigation requires more time to determine the nature and circumstances of the content, or where consideration of an appeal from the party whose content is to be removed is required.

It should also be noted that the German NetzDG, which is often cited as a model for a 24-hour removal approach, only requires removal of 'manifestly unlawful' content within 24 hours. For content that is unlawful but not 'manifestly unlawful', providers have a seven-day deadline to remove or block access to the content. We also highlight that the NetzDG only applies to a much more limited set of services and providers, i.e. it applies to profit-making internet platforms that are intended to allow users to share content with other users or make it publicly available, but it exempts platforms offering their own editorial content. The exemption also extends to 'platforms intended for individual communication or the dissemination of specific content' (e.g. WhatsApp, Gmail). The law also exempts games, and providers who have fewer than two million registered users in Germany.

Importantly, the German NetzDG clearly confines the content that is subject to removal to illegal content, i.e. content that violates one (or more) of 21 statutes of the German Strafgesetzbuch (StGB) (Penal Code). While the requirement to assess content against these 21 statutes is not without its (serious) problems, it at least provides greater certainty and less room for arbitrary interpretation compared to a concept of cyber abuse that is proposed in Part 7 of the draft legislation.

With respect to the proposed 24-hour period to implement website blocking request, ISPs believe that the implementation of such requests will be possible in most circumstances by larger providers. Much shorter timeframes are already being met for child exploitation material where these are being notified through automated AFP processes. Similarly, large ISPs have blocked websites giving access to terrorist material, e.g. the Christchurch attack, in much shorter timeframes.

However, smaller providers, which are captured by the draft legislation, may not have processes in place to receive and manually implement website blocks within a 24-hour timeframe over weekends or holiday periods. There may also be exceptional circumstances, such as natural disasters or other circumstances, that severely constrain operational capabilities, which may make it difficult even for larger ISPs to adhere to strict 24-hour timeframes.

In any case, it should be noted that any form of removal and website blocking stands and falls with accurate information on the material that is to be removed/blocked that must be conveyed with the initial notice and with the requisite technical expertise. (This comment does not in any way imply any judgement on the technical expertise of the Office of the eSafety Commissioner.)

3.7. Cyber-abuse material targeted at an Australian adult

Undoubtably, the internet provides access to material that some or even many users may find offensive. At the same time, modern democracies are based on freedom of expression, which can incur tension with a desire to eliminate offensive material online. Some will even go as far as advocating a right to offend. The French constitutional principle of laïcité arguably can be said to be based on this right.

Consequently, any definition of cyber-abuse material targeted at an Australian adult (CAMTAA) which embraces offensive material is likely to struggle to strike a balance between freedom of expression and protection from online harms.

The proposed definition for CAMTAA includes several components which must be satisfied:

- the material must be provided on a certain type of service;
- "an ordinary reasonable person would conclude that is likely that the material was intended to have an effect of causing serious harm" [3] to the adult under consideration; and
- "an ordinary reasonable person […] would regard the material as being, in all the circumstances, […] offensive"[4];
- with serious harm meaning serious physical harm or serious harm to a person's permanent or temporary mental health, with the latter including serious psychological harm and serious distress.[5]

We believe that this definition sets the bar too low and the scope is too wide. It is open to argument in relation to concepts such as 'ordinary reasonable person' and 'offensive'. Therefore, it does not strike an appropriate balance between guaranteeing freedom of expression and appropriately limiting online harms. Our concerns relate mainly to material that is deemed 'offensive', as opposed to material that is considered 'menacing' or 'harassing'.

While the concept of the 'ordinary reasonable' person is a well-known legal concept, it is doubtful that this concept can be applied effectively when combined with a judgement of what is 'offensive' as the latter is highly subjective. As numerous recent events have demonstrated, material that may be offensive to many members of a religion, including ordinary reasonable people, may not be offensive to other large parts of society (and even others within that same religion) – equally constituted of ordinary reasonable people. Indeed, Australia's own history demonstrates that some actions, current and historic, may be deeply offensive to some, but not all, ordinary reasonable persons.

The fact that the offensive material under consideration must be likely to be intended to have the effect of causing serious harm is only of very limited assistance in this context, given the very broad definition of serious harm, which includes a non-exhaustive list of mental conditions, such as psychological harm and serious distress, including temporary distress.

Unfortunately, Section 8 of the Exposure Draft also does not assist with an objective determination of what would constitute offensive material.

It is also not clear why likely intention is relevant in the assessment of CAMTAA. The material ought to be assessed objectively – by the ordinary reasonable person – and if that person concluded that the material would have the likely effect of causing serious harm, then, subject to the other criteria of the definition being fulfilled, the material would constitute CAMTAA. In our view, it is not useful to include intent into the test and the definition ought to be amended accordingly.

As highlighted above, we are also mindful of the overlap of material already subject to recourse under defamation law and CAMTAA.

Consequently, the proposed notice-and-removal regime for such content – or for any content prescribed under law for that matter – needs to be carefully considered and, in our view, often ought to be rejected as it risks moving jurisdictional and enforcement powers from the Courts to the eSafety Commissioner – something that is, independent of the person and office itself, not desirable in a democratic society.

We believe that an approach that limits the removal of material to illegal content is preferable. For example, the German NetzDG defines content to be removed by reference to statute (i.e. the German Penal Code) and seeks to minimise making decisions over online content by reference to common opinion or morality.

[3] Section 7(b), *Online Safety Bill 2020*, Exposure Draft
[4] Section 7(c), *Online Safety Bill 2020*, Exposure Draft
[5] Section 5, *Online Safety Bill 2020*, Exposure Draft

3.8. Abhorrent violent material

The Exposure proposes a new, dedicated power for the eSafety Commissioner to direct ISPs to block domains providing access to abhorrent violent material as defined in the Exposure Draft.

It is important to understand that ISPs did not receive such a direction (despite concerted efforts by ISPs to elicit such a direction), from the eSafety Commissioner, nor from any other authority, during and in the aftermath of the Christchurch terror attacks. In the absence of a direction to block the websites that hosted the footage of the shootings and the manifesto, all major Australian ISPs took the decision, at their own initiative, to block the identified websites. This left the ISPs exposed to legal liability – a situation which lasted almost 6 months.

Communications Alliance has since worked with the eSafety Commissioner to put in place a protocol that governs processes for website blocking for larger ISPs during online crisis events. The proposed notice power would complement this protocol, and we welcome the proposal in principle.

However, we raise concern with the powers of the eSafety Commissioner, on the basis that the definition of material that can give rise to blocking notices deviates from the definition of abhorrent violent material in the *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019* (AVM Act), i.e. the definition has been broadened in two material respects:

Firstly, the Exposure Draft provides the Commissioner with powers to grant blocking notices for material that 'promotes', 'incites' or instructs' in abhorrent violent conduct. However, it is not clear what criteria, if any, the eSafety Commissioner would apply to determine whether such material has such effects. From a rule of law perspective, this widening of the definition of material that is prohibited by statute, to material that is deemed sufficiently harmful to warrant blocking by the eSafety Commissioner, is concerning.

Secondly, the definition of abhorrent violent material pursuant to Section 9 of the Exposure Draft omits (among other details) the requirement of Section 474.31(c) of the AVM Act which, roughly speaking, stipulates that the abhorrent violent material under consideration is produced by the perpetrator or accomplice of the abhorrent violent conduct. In other words, the definition in the Exposure Draft broadens the abhorrent violent material definition to include any material produced by innocent by-standers, journalists etc.

We note that Section 104 of the Exposure Draft contains exemptions that mirror the defences available in the AVM Act, some of which cover material produced by a person working in a professional capacity as a journalist. However, material produced by by-standers, including original (first publication, i.e. not part of a news report) material exposing war crimes, police murders, etc., would as such not be covered by the exemptions and could be subject to blocking notices by the Commissioner. The AVM Act limited abhorrent violent material to material filmed by the perpetrator and accomplices for good reason – the considerations that led to this limitation ought to find equal application in the proposed Act.

Irrespective of which content is included or excluded in the definition, it is not useful to have two different definitions for the same term and within very similar legal contexts, i.e. website blocking. We urge Government to adopt the AVM Act definition of abhorrent violent material in new Online Content Act.

ISPs comply with a multitude of blocking request under various pieces of legislation. Communications Alliance and its members suggest that Government explores options for a centralised and automated flow of website blocking requests to Australian ISPs, similar processes used for the Interpol 'Worst of' list, to streamline the requests for website blocking from various Government agencies, to eliminate the potential for error and to reduce implementation timeframes.

We also note that the compensation arrangements on a no-profit, no-loss basis as available under Section 314 of the *Telecommunications Act 1997* are missing from the Exposure Draft and ought to be included.

3.9. Governance, appeals and transparency

Communications Alliance commend the Office of the eSafety Commissioner for the extensive educational, research and outreach work it has undertaken in the past years. We believe that the Office, being an independent statutory Office, is well placed within the broader communications and media remit of the Australian Communications and Media Authority (ACMA).

In principle, we do not object to some broadening of the powers for the Commissioner, including some of the removal/blocking notice powers.

However, it appears that the governance, appeals and transparency arrangements that underpin those powers ought to be strengthened.

For example, appeals for decisions of the Commissioner can only be made to the Administrative Appeals Tribunal (AAT).[6] This limited avenue for recourse for providers (and end-users) is disproportionate to the civil penalties envisaged in the Exposure Draft. It would be more appropriate and practical (also for the AAT) if the Online Safety Act provided for an internal review of a decision by the eSafety Commissioner. Internal review processes are not unusual – for example, the National Disability Insurance Scheme requires that an internal review be undertaken prior to a matter being escalated to the AAT.

Given the importance of the Office for the freedom of expression in Australia, it is imperative that the new powers envisaged for the Commissioner are balanced by appropriate governance arrangements. It is not quite clear what those arrangements will be, and we would welcome further discussion in this regard.

Also, this existing provision of the legislation that indicates the law should not be read as contravening the implied freedom of political communication (Section 233) does not provide a strong enough imperative for the Office to consider the implications of removing a piece of material.

At the very least, the Commissioner ought to be required to produce and table in Parliament an annual transparency report, detailing complaints the Office received, by category, all formal – and informal – requests and removal notices the Office has issued, the blocking requests and notices it has issued etc. This report could be similar in nature to the report produced by the Department of Home Affairs on the operation of the *Telecommunications (Interception and Access) Act 1979*. This report ought to be tabled no later than three months after the end of the reporting period to avoid undue delay and to allow for appropriate scrutiny.

3.10. Limitations of liability for voluntary action

We welcome the protections from civil proceedings and the limitations of liability for damages afforded by Sections 221 and 222 of the Exposure Draft, respectively.

Consequently, we request that the new Act also provides for an express exclusion of liability, similar to section 230(c)(2) of the U.S. Communications Decency Act which provides for an exclusion of liability for "any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected".

[6] Section 220, *Online Safety Act Bill 2020*, Exposure Draft

3.11. Disclosure of information

Part 15 of the Exposure Draft provides for the disclosure of information to various agencies and authorities etc. We note that it is not clear how the Exposure Draft envisages to handle requests for disclose for user data where the user data under consideration is subject to the privacy law of another jurisdiction which may be breached by the disclosure of the data.

Generally speaking, it appears that some of some of the envisaged thresholds for disclosure of user data are quite low, and we would welcome further discussion on this matter.

3.12. Deletion and cession of services

The Exposure Draft proposes to give the Commissioner an entirely new class of powers: the ability to demand the cessation of entire services in Australia. The proposed changes to the Online Content Scheme would empower the Commissioner to issue 'deletion notices' to app stores and search engines (Section 124 and Section 128), or to apply for a Federal Court order that a service cease being provided in Australia if it has contravened a relevant civil penalty provision twice in the previous 12 months (Section 156 to 158).

These are significant powers justified for use as 'last resort' measures. The Government's Online Safety Legislation Reform Discussion Paper (December 2019) argued the power would be needed when the app/service in question was "systemically and repeatedly facilitating" the posting of harmful content.[7]

However, as drafted, the draft legislation enables the Commissioner to use the link or app deletion powers and to seek orders from the Federal Court to have the service shut down after only two instances of a service's non-compliance.

In the interest of proportionality and meeting the policy intent of combatting 'systemic' content issues, intermediaries like app stores and search engines should not be required to remove apps or links unless there has indeed been systemic and wilful non-compliance by the services, and removal by the intermediary is truly the last resort, after all avenues have been exhausted with the providers of the services themselves.

Intermediaries should also not be required to take down apps or links where there is a genuine dispute as to the validity of the notices, which is a matter for the Commissioner and service provider. The language in the Exposure Draft ought to be amended in the relevant sections to require at least two notices having been provided to the specific service provider under consideration and to ensure the Commissioner has appropriately addressed the take-down with the service provider before requiring intermediaries to remove content.

Sections 124(4)(b)(i) an& (b)(ii) and 128 (4)(b)(i) & (ii) could be re-drafted along the following lines:

> *The Commissioner gave to the app provider/service provider [as relevant] two or more removal notices…. and;*
>
> *the app provider/service provider [as relevant] failed to comply with those notices within a reasonable time (no less than 3 business days from confirmation of receipt of the notice) and failed to provide reasons for non-compliance or raise a genuine dispute regarding the notices.*

In the same vein, for services that are subject to the Online Content Scheme, the Commissioner should be required to make reasonable efforts to make sure notices are being sent to the correct company point of contact and seeking an acknowledgement of receipt. Businesses often operate many different services independently of one-another and internal compliance mechanisms will need to be set up to ensure notices are actioned by the correct team.

[7] p. 47, Online Safety Legislation Reform – Discussion Paper, December 2019, Department of Communications, Cyber Safety and the Arts

Service providers should also be given an opportunity to provide objections as to the validity of notices before becoming subject to civil penalties and before the Commission can apply for orders to the Federal Court. This could be achieved by the Commissioner and Industry working together on remediation efforts, which could be as simple as finding the right communication channels to serve notices. The validity of the notice is currently assumed, where this may not be the case.

For example, Section 109 (2) & 114 (2) could be re-drafted:

> *So far as is reasonably practicable:*
>
> *the Commissioner must undertake reasonable efforts to ensure the removal notice is sent to the provider in a form and at an address designated by it to receive such notices;*

Equally, Section 109 (1) (g) (i) 114(1)(g)(i) could read:

> *Do so within:*
>
> *1 business day after the Commissioner receives an acknowledgement from the provider that the notice was received, unless the provider reasonably objects to the validity of the notice, in which case, after the objection is resolved;*
>
> *Such longer period as the Commissioner allows.*

A new section for objections handling could be inserted, for example:

> *The provider may object to a removal notice on the basis that it is not validly issued pursuant to the [Section]. If the Commissioner and provider cannot resolve any dispute within 30 days from the provider acknowledging receipt of the notice, the provider will be deemed to have not complied with the removal notice pursuant to Section [111 or 116].*

Amend Section 111 or 116 to read:

> *Subject to [insert new Section above] a person must comply with a requirement under a removal notice given under section 109 or 110 to the extent that the person is capable of doing so.*

These amendments would still deliver the policy intent and ensure that a failure to object to or acknowledge receipt of the notice or remove the material from the service within 5 business days, constitutes a failure to comply with the notice.

The Commissioner's powers in Section 156 – 158 as contemplated should be proportionate to the outcome contemplated by the Exposure Draft: the cessation of online services. The Federal Court power should be amended to reflect the proportionality applied to the app and link deletion powers, namely to be explicitly only applicable to non-compliance with notices relating to class 1 material, rather than the entire content scheme as currently drafted. Reasonable implementation of these new powers is also key to these thresholds being proportionate. For this reason, the Commissioner's powers should be elevated to only relate to a service's wilful non-compliance with notices. The Exposure Draft ought to be amended to reflect that these powers are reserved for providers who have exhibited systemic non-compliance with class 1 notices and who have declined to engage with the Commissioner on an appropriate remediation strategy.

Further, the proposed test of whether a service represents a 'significant community safety risk' is subjective and ambiguous. There is no universally accepted definition or standardised scale of online harms. Ideally this should be replaced by a more appropriate test such as 'serious harm to the Australian community' and, to support the Federal Court in making this assessment, there should be a public consultation process with civil society and industry to determine a clear position on what online harms would be considered to meet this specific threshold. Given that the definition of harmful content will not be static, and will evolve in line with the development of social norms and technological advancements, this community

designed threshold will likely need to be intermittently revisited. At the very least, indications as to the meaning of this threshold should be included in the Explanatory Memorandum.

4. CONCLUSION

We look forward to further engaging with Government, the eSafety Commissioner and other stakeholders in pursuit of the mutual desire to ensure that the Australian community is well-equipped to safely enjoy online environments.

We welcome the proposal for Industry to create principles-based codes to deal with key aspects of the new online safety regime, and we stand ready to engage with all stakeholders to facilitate the required code development processes.

We are also keen to closely cooperate with Government to develop an education and awareness campaign for the Australian public to ensure that end-users are empowered and motivated to protect themselves, as far as possible, from online harms and practice responsible online behaviours.

Noting a number of issues that require further clarification and discussion, we welcome an ongoing dialogue with key stakeholders.

For any questions relating to this submission please contact Christiane Gillespie-Jones on 02 9959 9118 or at c.gillespiejones@commsalliance.com.au.

Published by:
COMMUNICATIONS
ALLIANCE LTD

Level 12
75 Miller Street
North Sydney
NSW 2060 Australia

Correspondence
PO Box 444
Milsons Point
NSW 1565

T 61 2 9959 9111
F 61 2 9954 6136
E info@commsalliance.com.au
www.commsalliance.com.au
ABN 56 078 026 507