COMMUNICATIONS
ALLIANCE LTD

Communications Alliance Submission

to the Department of Infrastructure, Transport,
Regional Development and Communications

Online Safety (Basic Online Safety Expectations) Determination 2021

Exposure Draft & Consultation Paper

10 November 2021

Contents

Communications Alliance

Communications Alliance is the primary communications 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, platform providers, equipment vendors, IT companies, consultants and business groups.

Its vision is to be the most influential association in Australian communications, co-operatively initiating programs that promote sustainable industry development, innovation and growth, while generating positive outcomes for customers and society.

The prime mission of Communications Alliance is to create a co-operative stakeholder environment that allows the industry to take the lead on initiatives which grow the Australian communications industry, enhance the connectivity of all Australians and foster the highest standards of business behaviour.

For more details about Communications Alliance, see http://www.commsalliance.com.au.

1. Introduction

Communications Alliance welcomes the opportunity to make a submission to the Department of Infrastructure, Transport, Regional Development and Communications (Department) Exposure Draft of the *Online Safety (Basic Online Safety Expectations) Determination 2021* (BOSE) and associated Consultation Paper.

We lend our in-principle support to the BOSE and regard them as a useful means to foster a more uniform and consistent approach to online safety in the industry, and we agree with Government's general intentions.

However, we are concerned with the way that the BOSE, as currently drafted, could find practical application and fear that they even have the potential to undermine online safety and the security of the internet.

We would welcome further discussion with the Department and all relevant stakeholders.

2. BOSE as they apply Relevant Electronic Services and Designated Internet Services

BOSE as they apply to providers of email, SMS and MMS services in their capacity as carriage service providers and OTT SMS/MMS platform providers

2.1. The BOSE apply to social media services, relevant electronic services (RES) and designated internet services (DIS) of any kind. Relevant electronic services comprise email services, instant messaging services, SMS and MMS services, chat services and services that enable end-users to play online games with each other.

2.2. By and large, the BOSE target limiting the provision of or access to certain online content, i.e. 'material' that is unlawful or may be harmful, and actions that are required of service providers subsequent to the identification of such material (e.g. reporting, record keeping, complaint handling etc.)

2.3. Division 2 of Part 13 of the *Telecommunications Act 1997* prohibits the disclosure and use of information that relates to "the contents and substance of contents or substance of a communication that is being [has been] carried by a carrier or carriage service provider (including a communication that has been collected or received by such a carrier or provider for carriage by it but has not been delivered by it)" (Section 276). This means that these providers are prohibited (and also technically not set up to do so) to identify specific types of content carried over their services and to remove individual pieces of such content.

2.4. We have been advised by the Department that it is not the intention of the BOSE to create any friction between the requirements placed on providers of email, SMS and MMS services and the BOSE or, in other words, that there are no expectations that these providers detect, moderate or remove material described in the BOSE. We submit that this expectation be explicitly set out in the Explanatory Statement to the BOSE.

2.5. Consequently, large parts of the BOSE – to the extent we are able to define what is expected of providers – are not applicable to providers of email, SMS and MMS services in their capacity as carriage service providers, as compliance with the BOSE would imply a breach of obligations not to use the content and substance of a communication contained in Part 13 of the *Telecommunications Act 1997*.

2.6. Providers of email, SMS and MMS services are only able to limit access to certain types of content on these services (email, SMS, MMS) by limiting access to the service overall. With respect to SMS and MMS, this means that an access limitation to those services would also imply denying access to voice services, as it is usually not technically possible to separate access to voice from access to SMS/MMS services.

We note that this holds equally true for OTT providers of SMS/MMS platforms.

2.7. In the following, we comment on individual expectations as they specifically relate to providers of email, SMS and MMS services. We provide further comment on the expectations more broadly and in relation to other relevant electronic services providers, social media providers and designated internet services further below.

2.8. With regard to Expectation 6(3) and Core Expectation 11 in relation to SMS and MMS services, it worth noting that is not generally possible for providers of such services to remove individual pieces of communications from their networks. While it may on occasions be possible, under a local warrant or through the Mutual Legal Assistance Treaties (MLAT) process, to retrieve individual pieces of stored communications, it is not generally possible to do so at scale or to guarantee that such retrieval (and removal) is possible.

2.9. In relation to Additional Expectation 9 we note that providers of email, SMS and MMS services in their capacity as carriage service providers do not permit anonymous accounts, and cannot do so, due to a number of legal, regulatory and/or technical requirements and prohibitions. However, end-users can always avail themselves of free text-to-mobile websites (e.g. AnonTxt.com, Textforfree.net and Txtemnow.com) and other messaging platforms that allow users to send texts anonymously. Neither the relevant electronic service provider, nor the mobile carrier is in a position to prevent carriage and delivery to the end-user of this text.

2.10. With respect to Additional Expectation 10 (consultation and cooperation with other providers) and in relation to SMS, we highlight that the expectation bears a certain degree of overlap with work that Communications Alliance is already undertaking (in cooperation with the industry regulator, the ACMA), in relation to minimising scams via SMS (to the extent that the activities to do so are permitted by Part 13 of the *Telecommunications Act 1997*).

2.11. Given providers of email, SMS and MMS services are unable to reasonably minimise the extent to which the material listed in Core Expectation 11 is provided on their services, we believe it is an unreasonable and unnecessary regulatory burden and confusing for customers to expect those providers to make available complaint mechanisms specifically in relation to such material (Core Expectation 13)— when these providers have no ability to actually remedy the situation (i.e. to remove the material) other than to refer the customer to the Office of the eSafety Commissioner for further complaint escalation, or to advise to delete the material from the end-user account/device and possibly to block the sender from contacting them again.

Customers can, of course, make use of the usual complaints processes of these providers.

In relation to their role as providers of carriage services, we note that with respect to abhorrent violent material, internet service providers will be required to have processes in place to respond to blocking requests and notices from the eSafety Commissioner.

2.12. On the basis of the above, it appears that the means for providers of email, SMS and MMS services to minimise the extent to which certain material is provided on their service, and to 'ensure' that their services are 'safe', largely lie in developing (to the extent not already existent) terms and conditions/acceptable use policies for their respective services. However, it has to be clear that the enforcement of these policies would be dependent on an objective finding that a breach of the policy has actually occurred – something that may be, depending on the type of material, very difficult or even impossible to establish – and this could result in disputes between providers and their customers, and possible civil liability for the providers.

Application of the BOSE to certain types of chat services

2.13. The BOSE (and the *Online Safety Act 2021* (Act)) apply to "a chat service that enables end-users to communicate with other end-users" (Section 13A of the Act).

Irrespective of the arguments whether private over-the-top (OTT) communications are usefully included in the Act and BOSE, it is, in our view, clear that certain types of chat services ought to be excluded in the application of the BOSE (and the Act), on the basis that no or a very low risk of harm emanates from their use. Such services include, for example, chat services that are used to enable customer help and sales functions.

Application of the BOSE to OTT email, instant messaging and chat services

2.14. While providers of OTT email, instant messaging and chat services are not subject to the disclosure and use prohibitions of Part 13 of the *Telecommunications Act 1997*, they face similar difficulties of detecting and removing specific types and individual pieces of content in private communications of their customers.

Independent of the technical and potentially legal difficulties associated with the detection, analysis and removal of content, we maintain that any such activities would be inappropriate for private communications (refer to our submission in response to the Exposure Draft of the *Online Safety Bill 2020*).

2.15. 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 with the sharing of such content through public platforms accessible by a large number of individuals. In addition, private messaging services typically offer more granular controls that enable the user to protect themselves from such harm.

2.16. Importantly, how would providers of such services determine, in the context of a private communication between two individuals, whether the material in the communication meets the (undefined or loose) criteria for cyber bullying or abuse, whether the material was shared consensually etc., without extensive knowledge of the context and background of that communication?

2.17. As with SMS/MMS and email services provided by carriage service providers, providers of OTT email, instant messaging and chat services usually are unable to remove individual pieces of content from their services. These could lead to the risk of being required to block extraneous content, especially for services where the only avenue for the provider of the service to limit access to that specific piece of content is to deny the customer access to the account, noting that doing so could only happen on the basis of either an allegation by one party or investigation of the circumstances within a very limited remit, given the private nature of the communication (and the limited resources of a provider).

2.18. As with providers of email, SMS and MMS services, it appears that providers of OTT email, instant messaging and chat services would be limited to developing (to the extent not already existent) terms and conditions/acceptable use policies for their respective services to seek to ensure that their services are 'safe'.

2.19. With respect to Core Expectation 12 that requires providers to "take reasonable steps to ensure that technological or other measures are in effect to prevent access by children to Class 2 material provided on the service", we note, in line with our comments further above, that this is not a realistic expectation. Applying age restrictions to user-generated content is much more challenging than applying similar restrictions to films, movies or books where the producer has full control and authorship over the content. We also note that films, movies and books undergo a formal content classification process. Given the inability to control content on, for example, OTT email services, the only option to ensure that children are prevented from having access to Class 2 material would be not to provide them with the service.

In this context, we also note that almost every Australian student as of Year 3 (if not earlier) has and uses a school-based email account (of the type *first name.last name@school.education.state.gov.au* or similar) for home learning etc.

If the intention of the expectation is to say that if a service is designed, or if the service's terms of use generally allow, for the communication of Class 2 material, then providers ought to take steps to prevent children from accessing that material on the service, then the drafting ought to reflect this.

As currently drafted, no email provider (including the Department of Education) would be in a position to comply with the expectation to ensure that every child is prevented from accessing Class 2 material, if a user deliberately or unintentionally was to communicate such material in an email to a child.

The same comments apply to (widely used) chat and messaging services employed in classrooms across the country, such as Microsoft Teams, Google Classroom etc.

2.20. The same comments as set out in paragraph 2.11 above in relation to Core Expectation 13 (mechanisms to report and make complaints about certain material) apply to OTT email, instant messaging and chat services. As these providers are unable to reasonably minimise the extent to which the material in question is provided on their services, it may not be helpful to suggest to customers that a complaint to these providers is likely to trigger action (with the exception of complaints about Class 1 and abhorrent violent material) that would provide meaningful relief for the customer. The only means to remove the material from these services usually lies in an account closure/suspension – a measure that could result in providers opening themselves up to civil liability when they have, by and large, no ability to judge whether the alleged material is of the kind suggested or an activity has taken place as alleged.

2.21. As highlighted above, with respect to Class 1 and abhorrent violent material, it is not so much a specific complaints mechanism that is required, but rather processes on the provider's side to ensure that any such complaint results in the required actions (including escalations to the eSafety Commissioner and other relevant authorities) in accordance with the relevant legislation and regulation.

BOSE as they apply to Designated Internet Services

2.22. As the definition of DIS is so broad and includes any website, including any website that offers any form of commenting function, it is almost impossible to offer meaningful feedback on the types of difficulties that may arise for this category of providers. We believe that many, if not all, of our comments made in relation to other providers will equally hold for DIS.

General applicability of the BOSE to RES and DIS

2.23. Against the feedback submitted in this chapter, we urge the Minister to consider not making a BOSE Determination that applies to RES and DIS as the instrument, as current drafted, simply does not find meaningful application for these two sections of the industry.

It is worth noting that it was obviously also not the intention to capture these two sections of the industry under the BOSE as both the Policy Options and the Impact Analysis discussed in the Explanatory Memorandum to the *Online Safety Bill 2021*[1] specifically state that the BOSE would only apply to social media companies and model the cost analysis accordingly.

Consequently, we would like to see and understand a clear rationale and cost analysis that justifies the expansion of the BOSE, in what we believe is an ill-suited manner, to those sectors.

[1] p.30 and p. 35, *Explanatory Memorandum to the Online Safety Bill 2021*

3. General remarks

Commencement of the BOSE

3.1. The BOSE are to commence immediately upon registration of the Determination. While the Determination in and by itself does not impose a duty that is enforceable by proceedings in a court (refer to Section 45(4) of the Act), the eSafety Commissioner has the power to 'name and shame' providers that have, in her view, contravened one or more BOSE for the respective service that they supply (Section 48(2) and (3) of the Act).

The Act does not specify any timeframe that would be appropriate for the Commissioner to allow for implementation of the BOSE. Consequently, it remains at the Commissioner's discretion when she wishes to exercise her right to request, by written notice, periodic or non-periodic notices and to 'name and shame' as a result of the information that has been provided to her – and it remains at her discretion to allow (or disallow as the case may be) a certain 'grace period' for providers to implement what might be complex processes or technical measures required to fulfil the BOSE.

Moreover, as the Australian public will – understandably – not delve into the legal intricacies and interdependencies between the BOSE and the Act, it is likely to expect immediate compliance with the BOSE. This creates a mismatch of community expectations and technical compliance realities.

Given the extraordinary discretionary powers afforded to the Commissioner, the lack of clarity of what is required of providers in some respects and the far-reaching nature of other expectations (see further below for further commentary), we request that the BOSE only commence 6 months after registration and, thereby, provide some certainty to providers.

Lack of clarity and certainty for providers

3.2. Core Expectation 6(1) asks providers to "take reasonable steps to ensure that end-users are able to use the [respective] service in a safe manner." This expectation raises the following questions/concerns:

- How is 'safe' defined in this context? The concept of safety is subjective – while one user may feel safe, another user (of the same objective category of vulnerability) may not share that feeling.
- Providers are expected to minimise material or activity on the service that is or may be harmful. This is again a subjective and vague expectation. Not only is the expectation broadened to include material that may be unlawful and harmful (instead of actually being unlawful or actually being harmful), it also rests on the undefined term of 'harmful'. The term is neither defined nor used in the Act and bears the same issues of subjectivity as the term 'safe' as outlined above.

  Given the central nature of the term, we propose the term be defined for the purpose of this instrument to mean material that is not illegal, but with regard to which the eSafety Commissioner has powers under the Act, i.e. cyber-bullying material, cyber abuse material and material in relation to intimate image-based abuse.
- The lack of clarity and certainty is also concerning for providers as Section 221 of the Act specifically excludes liability for actions taken as a result of a remedial notice or a removal notice (and other notices) from the eSafety Commissioner, however these exclusions of liability do not extend to actions taken voluntarily and in good faith by providers to proactively remove material from their services.

- The lack of clarity of what is expected is even more concerning given that providers are expected to ensure that end-users are able to use the service in a 'safe' manner.

3.3. Furthermore, this unrealistic expectation of ensuring complete safety is coupled with a lack of a 'safe harbour' or some sort of 'deemed to comply' approach that would give providers certainty that their efforts are indeed meeting the expectations and would, therefore, not result in them incurring civil liability for good faith actions taken to comply with the expectations.

While expectation 6(3) lists a (non-exhaustive) number of 'reasonable steps' that could be taken to 'ensure' that services can be used in a 'safe' manner, taking some, or even all, of these steps does not seem to guarantee compliance with Core Expectation 6(1) as Core Expectation 7(1) indicates that the providers will need to consult with the eSafety Commissioner "in determining what are reasonable steps for the purposes of [Core Expectation 6(1)]".

Not only do providers have to consult the Commissioner, they also must have regard to any relevant guidance material made available by her Office in determining what are reasonable steps (Additional Expectation 7(2)).

3.4. The Consultation Paper correctly notes that "Service providers are best placed to identify these emerging forms of harmful end-user conduct or material, and so the flexibility of this regime means that providers and choose the best way to address them on their service in the most responsive way. The instrument provides examples of reasonable steps that could be taken to ensure safe use."[2] We agree with the Consultation Paper's assessment that service providers are best placed as to what reasonable steps to take to enable a safer use of the service, noting that we reject the notion that it will be impossible to ensure that end-users enjoy a '100% safe' environment, depending on the definition of safety.

We are, however, alarmed by the substantial discretionary powers that Core Expectation 7(1) grants to the Office of the Commissioner. While the Consultation Paper suggests that the service providers' expectation to consult with the Commissioner could be discharged by "seeking the advice of the Commissioner" or "following guidance issued by the Commissioner"[3], we are concerned that, in practice, the Commissioner will exert a far greater influence on what will be considered 'reasonable steps' and, therefore, when service providers will be deemed to have met the expectations.

This is of particular importance as the Commissioner herself has been assigned the powers to judge whether a provider has contravened one or more BOSE (Section 48 of the Act). (It is already extraordinary that the Commissioner has the power to 'name and shame' on the basis of a set of expectations, rather than on the basis of actual legal requirements.)

It is also not clear how a provider is expected to proceed in the (not unlikely) scenario where a provider and the eSafety Commissioner have differing opinions and/or guidance as to what would constitute 'reasonable steps' to 'ensure' that end-users are able to use the service in a 'safe' manner.

3.5. We are also concerned that the advice that the Office of the eSafety Commissioner will be providing in bilateral and confidential communications to individual providers will, over time (and potentially rather quickly) lead to diverging advice and practice.

[2] p.3, Department of Infrastructure, Transport, Regional Development and Communications, *Draft Online Safety (Basic Online Safety Expectation) Determination 2021 Consultation Paper*, July 2021
[3] ibid

This not only bears the risk of an inconsistent approach but may also impact competition.[4]

3.6. It would also be helpful to get a better understanding of what exactly is being expected of providers with respect to 'prevention' of access to certain material or an activity occurring. In a briefing on their Position Paper *Development of industry codes under the Online Safety Act* (released 29 Sept 2021) (Position Paper), the Office of the eSafety Commissioner made it clear that the Office's interpretation of prevention did not imply that the material under consideration would never be accessible to end-users (i.e. no 100% prevention) and that prevention would extend to the 'swift removal of the material under consideration'. If the Department takes a similar approach, given that the Determination has legal status, it would be beneficial to sharpen the language in this respect to give providers a greater degree of clarity of what is required of them.

Children's services

3.7. We acknowledge that children ought to be afforded special protections. However, Expectation 6(3)(b) asks providers to apply the most restrictive default privacy and safety settings if the service is "targeted at, or being used by, children" [emphasis added]. Given children may randomly access or 'use' any app or service they can lay their hands on – in the vast majority of cases for a very short time and without any detriment as they are not capable of meaningfully engaging with the service or app or quickly lose interest in it – the inclusion of mere 'use' in the expectation is not useful.

3.8. Requiring the default privacy and safety settings of a children's service to be set at the 'most restrictive level' is not useful as this criterion is only informed by the range of options made available by that service, and not grounded in the appropriateness of those options. For example, if a service only has a single level of restrictiveness, it could arguably meet the threshold of the expectation even if the setting is not objectively restrictive.

Instead, it would be more appropriate to require that the privacy settings be, for example, commensurate with the age of the user group targeted by the service or as identified upon sign-up.

Encrypted services

3.9. As noted in many discussions around this topic and in relation to Additional Expectation 8, it will be critical to carefully consider how the expectations in relation to encryption can be balanced with the need for a framework that safeguards the freedoms and privacy of individuals, including the privacy afforded through encrypted communications. Given the wide-ranging interest in encryption across multiple Departments and portfolios, we suggest that the use and application of encryption be dealt with separate to, and outside of, the BOSE.

3.10. Helpfully, the FAQ provide some guidance on the current intention of Additional Expectation 8 by stating that "Providers of encrypted services are expected to proactively address and mitigate unlawful and harmful activity on their services. Reasonable steps might include a range of actions, such as detecting misuse through behavioural, account or online signals including routing information and metadata and closing accounts."

However, if the use and application of encryption were to remain in the BOSE, we strongly recommend including this guidance in the Determination itself, given the importance of the issue for the security of the communications and, therefore, the functioning of our society.

[4] The telecommunications industry is already experiencing similar issues (of diverging advice and practice which has now led to calls for uniform practices) in relation to bilateral advice and guidance provided by the Communications Access Co-ordinator (CAC) in relation to the administration of the Telecommunications Security Sector Reforms.

We would particularly welcome clarification within the Determination as to what measures would NOT constitute 'reasonable steps' to proactively address and mitigate unlawful and harmful activity on their service by providers.

Anonymous Accounts

3.11. Additional Expectation 9 requests that providers take reasonable steps to prevent anonymous accounts from being used to deal with unlawful or harmful material. At the same time, the expectation proposes identify verification as one possible reasonable step.

The expectation and the potential reasonable step appear contradictory: if an account is anonymous, then it can, by definition, not be subject to an identity verification.

We submit that this expectation is confusing and requires more definitional work and consideration of what exact practices are to be targeted, both with respect to the end-user facing aspect of posts and the underlying subscriber/account/transactional data that the providers of the respective services hold.

For example, providers of relevant electronic services and social media services require account creation before being able to use these services. Identity verification is not required for many of these services, however subscriber data and transactional data can be disclosed subject to legal process. It should also be noted that Australian Privacy Principle 2 requires that individuals must have the option of not identifying themselves, or using a pseudonym, when interacting with entities regulated by the *Privacy Act 1988*.

Consultation and cooperation between providers

3.12. Additional Expectation 10 asks providers to "consult and cooperate with providers of other services to promote the ability of end-users to use all of those services in a safe manner."

Many providers already form part of substantial industry collaboration arrangements, e.g. through the GIFCT or the Technology Coalition. However, while Section 10(2) gives some examples of which reasonable steps may be taken to deliver cooperation – which may be problematic by themselves – it remains unclear what would constitute 'consultation and cooperation' for the purpose of the expectation and, therefore, constitute compliance with the expectation.

3.13. Beyond the definitional question of what level of consultation and cooperation may satisfy the expectation, it is unclear how the expectation could be translated into a functional/operational context without undue or undesired intrusion into users' privacy, conflict with international privacy law or freedom of expression: how are platforms' moderation practices to take into account activities on other platforms without potentially being regarded as interfering with freedom of expression, particularly in the context of political expression? We suggest that this expectation should explicitly enable collaboration across the industry but not require it.

Our members support the general intent to minimise bullying and harassment, including through volumetric attacks (pile-on attacks). We would welcome a more detailed discussion with the Department on the desired outcomes that this expectation is aiming to achieve so that providers can provide feedback on potential approaches to implementation that limit, to the largest extent possible, any inherent tension between content moderation and intrusion on freedom of expression.

Other comments

3.14. Expectation 6(3)(c) aims at ensuring that relevant personnel engaged in providing the service are trained in, and are expected to implement and promote, online safety. However, as currently drafted, the expectation could be read to target all employees providing the service, including those ancillary to the online safety aspects of the

service. It should be made clear that only those employees who hold functions relevant to online safety are required to be trained accordingly.

3.15. Additional Expectation 16 requests that providers ensure that information and guidance on how to make a complaint to the Commissioner, in accordance with the Act, is readily accessible to end-users.

As noted above, we agree that this would be very useful for services where the provider of the service has very limited or no means to remediate the problem, i.e. to remove content. However, this may be less useful or even counter-productive in situations where end-users are encouraged to first contact the provider of the service to address the content under consideration before turning to the eSafety Commissioner. Indeed, we note the eSafety Commissioner's position put forward in her recent Position Paper: "Industry participants will handle reports and complaints about Class 1 and Class 2 material and codes compliance in the first instance. eSafety will act as a 'safety net' if resolution of a complaint is not satisfactory."[5] The Act itself also stipulates a clear expectation that complaints first be made to the respective service providers.

Consequently, we recommend making it clear – for those providers that are in a position to remove material – that the expectation is not to make this information available at the same hierarchical level as complaint information for their own services, i.e. it ought to be made clear to end-users that complaints be directed to the provider of the service in the first instance.

3.16. Addition Expectation 18 asks providers to ensure that end-users receive regular reminders of and updates in relation to changes to information on terms of use, standards of conduct and policies as well as information in relation to online safety and parental control settings, including in relation to the availability of tools and resources published by the Commissioner.

We acknowledge the intention of the expectation to keep customers informed about tools and settings available to them to manage their or their children's' access to specific online material. However, while providers update their customers about changes to key documents – also for legal reasons – it is fair to say that the majority of customers does not engage with these communications or indeed find them 'annoying'. It is, therefore, questionable whether additional periodic reminders would be useful or could potentially even be counter-productive and disengage consumers. A number of studies have shown that consumers already suffer from 'information overload' and further periodic reminders of this kind are likely to contribute to this phenomenon.

Against this background, we suggest revisiting the discussions that our sector already commenced with the Department and the Minister's Office in 2020 to develop a national TV messaging campaign, similar to the Digital Switch-Over or the Slip-Slop-Slap campaigns, to push the relevant messages through appropriate channels on a large scale with Government backing. We have already developed (in consultation with the eSafety Commissioner) some messages that we believe can be applied across all types of online providers. We note the $5.2M provided for in the 2021-22 Federal Budget for a national Online Safety Awareness Campaign. We would welcome further discussion with the Department and relevant stakeholders on how to build on the existing work in this context.

3.17. Additional Expectation 19 asks providers to keep records of reports and complaints about material for 5 years after the making of the report or complaint to which the record relates. However, in the absence of a preservation order, many providers do not keep any communications of users when the users delete their accounts,

[5] pp.5/6, eSafety Commissioner, Development of industry codes under the Online Safety Act, Position Paper

irrespective of whether a complaint once may have been filed in relation to the users' communications.

Doing so would require substantial platform re-engineering and would involve significant costs where it can be done at all. It would be useful to understand what exactly providers are expected to record and store and for what exact purpose.

We are also usure if keeping substantial amounts of potentially personal data for prolonged periods of time is in the user's interest or aligns with privacy law/best practice.

3.18. Additional Expectation 21 envisages that an individual who is an employee or agent of the provider be nominated as the contact person for the purposes of the Act and be notified to the eSafety Commissioner.

We welcome clarification as to what is meant with 'for the purposes of the Act' in the context of 24-hour removal notices that may be received from the Commissioner. It needs to be clear that the nominated contact person will not be available 24/7 to receive removal notices and to act on those. These functions will be fulfilled by numerous personnel designated for that purpose and cannot be assigned to a single individual.

An alternative and better approach would be for the Additional Expectation to require a provider to have a single contact point (e.g. an email address or a contact number that leads to the appropriate department within the provider and which can be staffed 24/7) instead of a single contact person.

BOSE are not basic and substantially expand the remit of the Act

3.19. Lastly, it is important to note that the name Basic Online Safety Expectations is, in our view, a misnomer as the name appears to suggest that compliance with the expectations would require only a basic level of effort or measures from providers or set a minimum standard for compliance.

In reality, some of the core (and additional) expectations go well beyond any basic measures and international best practice. For example, the notion that providers could share volumetric data across platforms with relative ease (Additional Expectation 10(2)(a)) is incorrect. Doing so would require specialised technical expertise and process reengineering. It may also require organisations to disclose commercially sensitive or proprietary information.

3.20. The fact that the BOSE do not impose a duty that is enforceable by proceedings in a court cannot detract from what seems to be an intention to substantially extend the Act from a 'notice and take-down' regime to a 'detect, moderate, report and remove' regime.

4. Conclusion

Communications Alliance looks forward to continued engagement with the Department and other relevant stakeholders on the important topic of protecting all Australians from dangerous or inappropriate online content.

We continue to lend our support to the overarching objectives of online safety expectations for the communications sector and stand ready to work with all stakeholders to facilitate an effective and efficient adoption of such expectations, alongside with the *Online Safety Act 2021* and Industry Codes, in our sector.

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