UTS

CENTRE FOR MEDIA TRANSITION

Online Safety Legislative Reform

Discussion Paper, December 2019

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

DATE: 21 February 2020

About the Centre for Media Transition

The Centre for Media Transition is an interdisciplinary research centre established jointly by the Faculty of Law and the Faculty of Arts and Social Sciences at the University of Technology Sydney.

We investigate key areas of media evolution and transition, including: journalism and industry best practice; new business models; and regulatory adaptation. We work with industry, public and private institutions to explore the ongoing movements and pressures wrought by disruption. Emphasising the impact and promise of new technologies, we aim to understand how digital transition can be harnessed to develop local media and to enhance the role of journalism in democratic, civil society.

This submission was prepared by:

- Dr Karen Lee
- Professor David Lindsay
- Dr Sacha Molitorisz
- Dr Derek Wilding

Contact

Centre for Media Transition
Faculty of Law, University of Technology Sydney
Building 2, Level 15
UTS City Campus, Broadway
PO Box 123, Broadway NSW 2007

cmt@uts.edu.au
+61 2 9514 9669

cmt.uts.edu.au

1. Introduction and general principles

Thank you for the opportunity to contribute to this review.

Our submission addresses several of the questions put by the Department. As our responses are arranged thematically rather than in the order in which they are presented in the Discussion Paper, below is a list of the points we address in this submission and the corresponding questions.

1.	Introduction and general principles	N/A
2.	Connecting with other legislation	Various questions
3.	The objects of this Act	Questions 1 and 2
4.	Regulatory obligations versus expectations	Questions 3 to 6
5.	Extending regulatory obligations	Questions 7 to 10 Questions 11 to 15 Questions 16 to 18 Questions 19 to 23 Questions 28 to 30
6.	Key concept: seriously harmful content	Questions 19 to 23
7.	Use of co-regulation	Questions 19 to 23
8.	Governance and resources	Questions 36 to 39

The ACCC's Digital Platforms Inquiry has provided guidance on the points at which platforms should be brought within the regulatory framework, and we are pleased to see the Government's Implementation Roadmap offers a plan for approaching this task, with the proposal for an Online Safety Act one of the first initiatives.

We recognise the proposed legislative changes are an important step in legislative reform. Our comments in this submission are intended to help strengthen aspects of the online safety regime by retaining effective existing regulatory concepts and mechanisms while developing new approaches to deal with the challenges of technology, industry practice and community expectations. As some of the existing provisions in Schedules 5 and 7 of the *Broadcasting Services Act* 1992 (BSA) are complicated and are part of interlocking arrangements that operate across other legislative schemes, we suggest the proposed changes be the subject of a further round of consultation, perhaps in the form of an exposure draft of the new Act, before being introduced to Parliament.

Summary

At the outset, we note there is much to support in the proposed reforms, particularly in relation to image-based abuse and cyberbullying.

We support in principle the following proposals, noting that some matters require further information or clarification, and that some qualifications are added in sections 2 to 8 below.

- the reduction of response times for take-down notices from 48 hours to 24 hours;
- the removal of distinctions between hosting services, live content services and links services;
- the extension of mandatory removal notices for cyberbullying material to other platforms and services such as gaming, messaging and social connection sites;
- the extension of regulation of cyber abuse to adults (with adults required to satisfy a test that is more restrictive than that applicable to minors);
- the extension of the eSafety Commissioner's powers to issue take-down notices if certain material is accessible to Australians, irrespective of whether the content is hosted overseas;
- the proposal to provide the eSafety Commissioner with additional tools (such as infringement notices) for cyberbullying and image-based abuse;
- reviewing and where necessary updating the codes developed under Schedules 5 and 7 of the BSA;
- the proposition that obligations on ISPs (and to this we would add digital platforms) should be different to those imposed on content providers;
- a principles-based approach to code formation, provided the codes remain enforceable.

On several other points we have serious concerns, also explained in sections 2 to 8 below:

- the categorisation of services such as social media services will not address inconsistencies and uncertainty in existing legislation, and may also be internally inconsistent;
- the shift to a 'harm' based approach in regulating online content may erode longstanding principles that generally promote freedom of expression, with restrictions and prohibitions imposed where needed;
- though it is not clear from the Discussion Paper, it appears that social media (and other online platforms and applications) will become subject to the online content scheme which imposes restrictions on MA15+ and R18+ content;
- the relationship between 'seriously harmful content' and the higher end of the classification ratings (X18+ and RC) is not sufficiently clear;
- delinking decisions of the eSafety Commissioner from the National Classification Code and the Classification Board undermines the role of the Board in setting the benchmark for community standards, against which various industry schemes, tools and practices can be compared;
- establishing the office of the eSafety Commissioner as an autonomous accountable authority under the *Public Governance, and Accountability Act 2013* (PGPA Act) could lead to less accountability in decision making and inconsistency with related activities of the ACMA.

Principles

Some general principles have guided the development of our response to this consultation.

1. Online content regulation requires a proportionate approach that balances protection from harm against other rights and interests, including freedom of expression, privacy and autonomy.
2. Digital platforms should be brought into the regulatory framework at appropriate points but there is a need for consistency in how they are characterised across legislative schemes.

3. Digital platforms are not, for the most part, primary publishers of content; while it is appropriate to impose regulatory obligations on them, these obligations will be different from those of publishers.
4. New arrangements facilitating rapid responses to urgent events and harmful content are needed; however, decisions on content categorisation should be linked to and reviewable under the National Classification Scheme.
5. There should be consistency in the approach to extra-territorial application of Australia's laws.
6. Regulatory obligations should be enforceable; if the associated conduct does not require enforcement by a regulator, it should be the subject of industry self-regulation.
7. Regulatory governance should be consolidated, not further fragmented, maximising the opportunities for cooperation, transparency and oversight.
8. Modernising the regulatory framework to take account of digital platforms is an opportunity to address other longstanding problems in communications regulation.

Finally, we note that on some important matters, it is difficult to reach an informed view on the proposal without more detail on its design or operation. This is the case, for example, on the transposition of co-regulatory arrangements to the proposed new online content scheme.

2. Connecting with other legislation

Various questions posed by the Discussion Paper.

While the proposed Online Safety Act is important mainly for its potential to protect Australians from harmful online material, it is also significant for its treatment of digital platforms and other service providers. As the ACCC noted in the Final Report of its Digital Platforms Inquiry, and as the Government recognised in its response, the conduct of digital platforms can be difficult to place within the existing regulatory frameworks. While some activities are governed by competition law, consumer protection, communications law, data privacy, copyright or defamation, there is uncertainty over the extent to which some activity is captured by existing law, and there are some aspects that are not regulated.

In submissions to the Digital Platforms Inquiry, the Centre for Media Transition took the approach that digital platforms – at least in respect of their current activities – are not direct 'publishers' of content and should not be regulated in the same way as broadcasters or other news publishers. Nevertheless, we have consistently advanced the view that they should be brought within the regulatory framework at appropriate points.

This task is complicated by the fact that 'digital platform' is a convenient term used for businesses that provide very different services; indeed, their activities vary considerably even within the one overall business entity. For instance, Google search cannot be equated with Google News, let alone YouTube. This is recognised in the proposal for a 'reserve power' to regulate 'ancillary service providers' (which we address in section 5 below). As the Online Safety Act is among the first attempts to adapt the regulatory framework to accommodate digital platforms against the background of the ACCC's findings, we think it is important that this crucial step of identifying the activities of platforms and giving them a legislative definition takes into account the other legislative contexts in which they must be recognised.

In short, this means describing the services digital platforms may offer, now and in the future, in a consistent way across the Online Safety Act, the BSA, the *Telecommunications Act 1997* (TA) and other Commonwealth legislation that recognises communications services (such the *Criminal Code Act 1995*), as well as in state and territory legislation (such as the uniform defamation laws, also under review). It is desirable that any terminology adopted in the proposed Online Safety Act is consistent with other work being undertaken by the Department to harmonise the communications regulatory framework.

We offer the following specific comments on the approach proposed in the Online Safety Act and how it connects with other regulation.

- Social media services such as Facebook and Twitter would not be the subject of a single definition across the Online Safety Act and the BSA. In the Online Safety Act – following the model for image-based abuse in the *Enhancing Online Safety Act 2015* (EOSA) – 'social media service' is one of three services (the others being a 'relevant electronic service' and a 'designated internet service') to which laws about posting intimate images apply. A social media service also meets the definition of 'online content service' in cl 3 of Schedule 8 of the BSA, meaning it is subject to restrictions about gambling advertisements, even though that Schedule does not explicitly mention a 'social media service'.
- A social media service is currently a type of 'content service' for the purposes of the abhorrent violent material scheme in Division 474 of the Criminal Code (see the definition at s 474.30). It would also meet the definition of 'hosting service' in cl 4 of Schedule 7 of the BSA, but may not be regarded as falling within Schedule because of the assumed absence of an 'Australian connection' (see discussion below).
- The introduction of the Online Safety Act provides an opportunity to rectify such inconsistencies, but it is difficult to ascertain from the Discussion Paper how content services under Schedules 5 and 7 of the BSA will be treated when the regulations are transferred to the Online Safety Act. On one reading of the Discussion Paper, the three part typology in the EOSA (ie, social media services, relevant electronic services and designated internet services) will be applied to the online content scheme. The reference on p 40 of the Discussion Paper to 'designated internet services' as among those to which the new codes would apply suggests that the EOSA categories will apply in place of the current Schedule 5 and Schedule 7 arrangements. This would mean that, in relation to content regulation, Facebook, Twitter etc would be covered by the same definition of 'social media service' used elsewhere in Online Safety Act. In effect, the catch-all function of the 'designated internet service' category means that almost any internet content and service that is not explicitly excluded – in the way, for example, that an 'on-demand program service' is excluded by the operation of s 9A(1)(e) of the EOSA – would be subject to the online content scheme. While that would help with consistency, it could have a serious impact on freedom of expression (see our comments in sections 6 and 7 below). An alternatively consistent approach may be to exclude 'social media services' (and other services) from the online content scheme.
- Apart from problems with consistency with the definition of services, a problem with the Online Safety Act proposals is that they appear to leave in place differing approaches to the extra-territorial application of Australia's communications laws. As noted above, it appears a reason that the online content scheme in Schedule 7 of the BSA may not apply to social media platforms is because the content is not necessarily hosted in Australia (ie, the service does not have an 'Australian connection'). While in policy terms it might be desirable to exclude social media from the online content scheme, relying on the likely absence of an Australian presence is not a sound basis for exclusion when the same service is subject to other forms of regulation in both the Online Safety Act and the BSA. In our view, this illustrates the need for a clearer typology of services and service providers that would offer clarity on regulatory obligations under the applicable Acts.
- If these definitional aspects can be addressed, we think the proposed removal of the distinctions between hosting services, live content services and links services and the resulting changes to take-down notices appear to be welcome improvements. However, we have some reservations about the category of 'seriously harmful material' (see our separate comments on this in section 6).
- As part of the difficulty in understanding the application of current law arises from the use of terms such as 'relevant electronic service' and 'designated internet service', which were developed specifically to apply to image-based abuse material, we recommend that the Department takes the opportunity to revise the terminology used in the EOSA, and wherever possible to use terms that are more likely to be recognised by consumers and members of the public who will be the subject of education and digital literacy campaigns.

- Similarly, we think it would be regrettable to characterise Google search, Bing search and similar services as 'ancillary service providers' (as proposed on pp 52-53 of the Discussion Paper) in the Online Safety Act, when such a term is unlikely to be useful in other Acts and will be incomprehensible to people unfamiliar with online safety regulation.
- The concept of an 'internet intermediary' is still useful. While we do not support the broad protection offered in the way of the Communications Decency Act in the US, we think it is reasonable to differentiate the curation and distribution activities of most digital platforms from the programming and content supply activities of broadcasters and publishers.

3. The objects of this Act

Question 1 and 2 (p 19).

We recognise that the main aim of this Act is to tackle a range of online material that the community expects would be prohibited or regulated in some way. While there would be broad agreement on the need to take action to discourage and to respond to material such as the live streaming of the Christchurch mosque killings, there is scope for disagreement on the kind of material that would be regulated at, for example, the MA15+ level. Nevertheless, the classification and online content schemes have managed this problem over a number of years. We are concerned that, in moving online content regulation from the BSA to the Online Safety Act, Australia may lose effective mechanisms that have been developed to protect freedom of expression even as they protect from harmful material. This point is addressed below in relation to the use of the National Classification Code, but it also arises in relation to the objects of the Act. We also note that several proposed statements of regulatory policy appear to be statements of objects, rather than policy.

- Likely as a result of the organising principle of 'safety' and of importing the online content regulation scheme into an Act dealing with image-based abuse, cyberbullying and cyber abuse, there appears to be a shift in Australia's well-established approach to content regulation that emphasises classification of content over censorship. This approach, founded on the principles in the *Classification (Publications, Films and Computer Games) Act 1995* (Classification Act), recognises the importance of freedom of expression, as evident from s 1 of the National Classification Code. This provision is as follows:

    1. Classification decisions are to give effect, as far as possible, to the following principles:

        (a) adults should be able to read, hear, see and play what they want;

        (b) minors should be protected from material likely to harm or disturb them;

        (c) everyone should be protected from exposure to unsolicited material that they find offensive;

        (d) the need to take account of community concerns about:

            (i) depictions that condone or incite violence, particularly sexual violence; and

            (ii) the portrayal of persons in a demeaning manner.

- In the BSA, there is a recognition of the need for a balanced approach in the Objects of the Act in s 1, which retain the important element of the reasonable adult along with material unsuitable for children:

    (l) to restrict access to certain internet content that is likely to cause offence to a reasonable adult; and

    (m) to protect children from exposure to internet content that is unsuitable for children.

- In contrast, in the proposals for the Online Safety Act, the only recognition of free expression is in one of the statements of regulatory policy:

- Balance the competing objectives of user safety and freedom of expression.

- In our view, there is a need for clear recognition of the importance the community places on freedom of expression and on adults being able to access material online. Such a statement should be a standalone object; it can then be taken into account alongside other objects, designed to protect against harmful content, when interpreting the provisions of the Act.
- Accordingly, we take a different view from that expressed in the *Report of the Statutory Review of the Enhancing Online Safety Act 2015 and the Review of Schedules 5 and 7 to the Broadcasting Services Act 1992 (Online Content Scheme)*. On p 15 of her report, Lynelle Briggs AO made the following observation.

> Reliance on a classification system that is focused, amongst other things, on allowing adults to make informed choices about what they read, hear or view is highly questionable when applied to children's safety. The eSafety Commissioner argues that the use of a harm standard would allow the online content standard to operate separately from classification policies and practices as well as allow for faster assessments of content.
>
> > "Such an assessment… would [prevent] access to content that is likely to do harm (eg preventing children accessing violent and degrading online pornography), or [prevent] access to content production which is harmful (eg child sexual abuse material)." [footnote omitted]
>
> Online content providers do not mind how material is classified, so long as it is done correctly, consistently and quickly, and does not vary between media or technology.

- We disagree with this approach because we think action to protect children's safety has always been the foundation of classification in Australia and while service providers might not mind how material is classified, the community might. Improving the ways in which those protections are enforced may well mean allowing swift and responsive initial decisions by an authority other than the Classification Board, but this should be done within a framework that recognises the importance of community standards generally and promotes other freedoms that Australians respect and value.

4. Regulatory obligations versus expectations

Questions 3 to 6 (p 25).

One component of the Online Safety Act comprises the 'basic online safety expectations'. We understand and support the Government's attempts to encourage industry participants to find ways of effectively protecting the community from unacceptably harmful online material. However, it appears to us that legislating for 'expectations' rather than obligations creates a new grey area that sits somewhere between self-regulation and statutory regulation, without the structure and accountability offered by codes of practice registered with a regulator. We feel this is unlikely to benefit either the service providers or the community. We understand there may be concerns about premature or over-interventionist approaches hampering innovation, but we think the choice should be between industry self-regulation, co-regulation with the oversight of a regulator, or government regulation. Specific comments on the provisions of the Online Safety Act are below.

- In relation to 'transparency reporting' for the basic online safety expectations, there are to be no sanctions for non-compliance, but the eSafety Commissioner would have the power to impose specific (enforceable) reporting obligations. If these obligations are not complied with, the enforcement action that could be taken is a public statement that a service provider is not complying with the basic expectations. It appears there is no subsequent step whereby a provider is, in fact, required to meet the expectations. The Discussion

Paper says that if industry efforts to meet the expectations are insufficient, the Government 'reserves the right to consider additional regulatory action to require compliance' (p 23). We strongly advise against this approach because it leads to a hollow regulatory scheme that cannot be enforced without legislative amendment, taking additional time and parliamentary resources.

- On p 20 of the Discussion Paper there is a comment on the importance of preventative measures to tackle online harms, with reference to the requirements imposed on social media services under the EOSA to establish a complaints scheme for cyberbullying material and to include in the service's terms of use a prohibition on posting cyberbullying material. It is not clear whether an approach such as this is to be adopted for other matters. It appears that the proposed approach to privacy and safety settings on apps and games (p 23) and the provision of point of purchase information (p 24) revert to the basic 'online safety expectations' approach under which the Government 'will consider' providing the eSafety Commissioner with the power to enforce obligations in the event that the expected standards are not reached. In our view, it would be more effective to provide a clear, legislative statement of Parliament's expectation that relevant service providers develop a code of practice dealing with certain matters, with the regulator deciding whether the code rules are adequate and having the power to adopt a mandatory standard if online service providers fail to adopt a code or if the code rules they propose are inadequate.
- We note that in its response to ACCC Digital Platform Inquiry Recommendation 18, the Government confirmed its commitment to introduce a binding privacy code that would apply to 'social media platforms' and that this would include specific rules to protect the personal information of children and vulnerable persons. To the extent that the safety measures proposed in connection with the Online Safety Act are not better accommodated within the new privacy code arrangements, there would clearly be a need for consistency across the two schemes.
- While we agree that safety by design is important (outlined at p 9 and pp 20-21 of the Discussion Paper), we note the importance of other regulatory objectives identified by the ACCC and the need to account for privacy and for further human rights including freedom of expression. There is a risk that other regulators, or the same regulators performing other regulatory functions, will engage separately with the same digital platforms on certain design aspects. For example, the Australian Human Rights Commission, in its Discussion Paper on *Human Rights and Technology* (Dec 2019) is proposing that the Australian Government establish a taskforce to develop the concept of 'human rights by design' in the context of AI-informed decision-making (Proposal 13, p 191). We encourage the Department to approach these aspects of design in a holistic way.

5. Extending regulatory obligations

Questions 7 to 10 (p 30)

Questions 11 to 15 (p 34)

Questions 16 to 18 (p 37)

Questions 19 to 23 (p 44)

Questions 28 to 30 (p 52)

As mentioned in section 2, we have argued in previous submissions for the extension of regulatory obligations to digital platforms, where appropriate, and preferably under a framework that maintains consistency in regulatory categories and services across different statutory schemes. We make the following comments on specific proposals to extend current regulatory arrangements.

- We support the extension of mandatory removal notices for cyberbullying material to other platforms and services such as gaming, messaging and social connection sites.
- We support in principle the extension of the eSafety Commissioner's powers in issuing a take-down notice if certain material is accessible to Australians, irrespective of whether the content is hosted overseas (but see our separate comments on 'seriously harmful content' in section 6, below). We note there may be practical difficulties in enforcing such action, but some service providers may comply voluntarily with take-down notices.
- We support the shortening of the response time for take-downs under the image-based abuse scheme and the cyberbullying scheme from 48 hours to 24 hours as well as the similar adjustments to the response times under the online content scheme. We think it would be appropriate to allow a service provider to seek an extension of time in extenuating circumstances (eg, if it is also responding to a major event such as a mass shooting). The existing arrangements in Part 10 of the EOSA for review by the AAT of a decision to issue (or to not issue) a 'social media service notice' should be maintained.
- We note the proposal to introduce civil penalties in relation to the adult version of cyberbullying referred to as 'cyber abuse'. We assume the intention is that this will apply to failure to comply with a notice (as is the case under s 36 of the EOSA), rather than to cyberbullying itself (in the way that contraventions of the image-based abuse rules arise from posting or threatening to post the material). In any event, we do not support the use of civil penalties for individual end-users who do not respond to take-down notices for adult cyber abuse. We think action against end-users for adult cyber abuse should primarily be a matter for criminal law. Improving laws relating to abuse, harassment, stalking – to the extent that this is needed – in conjunction with a take-down regime targeting service providers, would be preferable to the introduction of civil penalties. Further, on a practical level, the use of civil penalties would require an application to the Federal Court, meaning that enforcement action is costly and time-consuming and imposes a penalty on an individual without meeting the higher burden of proof required in a criminal prosecution. We think this proposal should be set aside.
- While we acknowledge the harm that can be caused by cyberbullying and cyber abuse, we have some reservations about the risks to free expression that could result from establishing a cyber abuse scheme for adults. We note the intention to impose a higher threshold for what constitutes cyber abuse, but one of the limbs of this test is that 'an ordinary reasonable person would, in all the circumstances, regard the material as menacing, harassing or offensive …' We think the inclusion of 'offence' may act as an undue restriction on speech, whether through action taken by the eSafety Commissioner or in pre-emptive removal of content by service providers.
- In addition, we are concerned at the extent to which the Online Safety Act places decisions on community standards in the hands of officials. In this case, decision-makers within the eSafety Commission, in addition to deciding whether standards such as 'serious distress or serious harm' are met, would make assessments of the intention of the person posting the material and the views of an ordinary, reasonable person. We would have more confidence in this change if such decisions were made in an environment where other commissioners or Authority members could be consulted or offer views. This informs our view on governance arrangements (see section 8, below).
- Further, we think there should be a specific mechanism for review of the decision that material is 'seriously harmful content', separate from the decision to issue a notice. This point is addressed in section 6 below.
- In principle, we agree with the proposal to provide the eSafety Commissioner with additional tools (such as infringement notices) for both cyberbullying and image-based abuse, but we seek clarification on the tools being considered.
- We think there is little value in a *statutory* power for the Commissioner to 'request' that a service provider enforce its terms of service against a user. We note that inclusion of certain provisions in a service's terms of use is an element of the basic online safety requirements set out in s 21 of the EOSA, and that while there is an accompanying statement in s 22(1) that Parliament expects services will comply with these expectations, there is also an explicit statement in s 22(3) that this 'does not impose a duty that is

enforceable by proceedings in court'. As noted in section 4 above, we do not support the statutory enactment of unenforceable obligations; in our view, obligations that do not warrant enforcement powers should be left to industry self-regulation. Further, we are also concerned that the reliance on providers' terms of service could lead to more onerous obligations being imposed on all users and to providers reserving rights very broadly against users, purportedly on the basis that they are 'required by law' to do so.

- Subject to review of its draft provisions, including review and oversight mechanisms, we support, in principle, the proposal for a new power in the Online Safety Act that allows the eSafety Commissioner, when dealing with an urgent situation involving terrorist activity or extremely violent material, to issue directions to ISPs to block websites for limited periods. But we are concerned that this proposal creates another type of content to which specific regulatory provisions apply.
- In summary, the 'high end' of harmful content under these various schemes would comprise the following:
    1. 'terrorist or extreme violent material' during an 'online crisis event' where ISPs will be subject to website blocking under the Online Safety Act;
    2. 'abhorrent violent material' for which the providers of content services and hosting services are subject to notices issued under the Criminal Code;
    3. 'seriously harmful material' for which a range of online services are subject to notices issued under the online content scheme in the Online Safety Act;
    4. 'RC' material for which ISPs, internet content hosts and other content providers are subject to rules under codes of practice and ultimately to the various kinds of take-down notices that can be issued under the Online Safety Act.
- This list does not include the material subject to regulation under the image-based abuse, cyberbullying and cyber abuse schemes in the Online Safety Act. Nor does it include the existing obligation on carriers and carriage service providers under s 313 of the TA to use their best efforts to prevent the use of networks and facilities in the commission of an offence and to comply with notices issues by the eSafety Commissioner under s 581 of that Act. As website blocking is the most interventionist response and the most likely to interfere with freedom of expression, we would not support its automatic extension to 'seriously harmful material'. However, it may be worth reviewing the relationship between the proposed Online Safety Act and the mechanisms established under the TA.
- Also in relation to the proposals for website blocking, we do not support the use of a statutory power to issue voluntary notices to ISPs. Situations involving dangerous content require a stronger response than a voluntary notice or even a formal warning to encourage future compliance. Further, while failing to adequately address serious online safety concerns, the issuing of a voluntary notice that will be made mandatory if not complied with has no substantive effect on freedom of expression.
- We note that the scheme regulating abhorrent violent material is to remain as part of the Criminal Code, even though the action taken under that scheme (apart from prosecution) is initiated by the eSafety Commissioner. An explanation of the rationale for this approach would be useful.
- As noted in section 2, we have concerns over the introduction of the term 'ancillary service provider' in the proposed Online Safety Act to characterise both internet search services and digital distribution platforms, when that term is unlikely to work in other legislative contexts and will not promote wider understanding of the scheme. More broadly, we do not support the introduction of another non-enforceable, statutory power to issue notices or another opportunity for the Minister to specify additional services subject to the scheme. More fundamentally, we are concerned about the restrictions of free speech that could arise from the introduction of a scheme that is, in effect, the equivalent of website blocking. We are especially concerned that the power could be used in relation to adult cyber abuse rather than just child sexual abuse material. The example given in the Discussion Paper is of overseas hosted material where the provider has little regard for Australian law, but it is not clear whether the power would only be exercised for overseas content. We think the introduction of this power requires further justification, including an explanation of the limits of its application and the meaning of 'systematically and repeatedly facilitating the posting

of'. The proposed Online Safety Act would give the eSafety Commissioner a range of tools to deal with harmful content, and the codes of practice to be developed under the online content scheme could be used to encourage digital platforms to continue to develop solutions without the need for regulatory intervention.

6. Key concept: seriously harmful content

Questions 19 to 23 (p 44).

We understand the intention is to bring together different aspects of regulation and create a more consistent and effective response, including in relation to content hosted outside of Australia, partly through the identification of 'seriously harmful content' in the online content regulation scheme. We agree with the approach adopted in the Discussion Paper under which MA15+ and R18+ and X18+ material does not fall into this category and is not covered by the escalated regulatory responses. Nevertheless, we are concerned about some aspects of the proposed arrangements.

- It is not clear from the Discussion Paper how regulatory provisions in Schedules 5 and 7 of the BSA that cover material *other than* seriously harmful material will be treated under the Online Safety Act. The Paper says that 'most elements' will be transferred to the Online Safety Act. We seek clarification on how this will operate.
- As noted in section 2 above, on one reading of the Discussion Paper, the intention is to apply to the online content scheme the three part typology in the EOSA (ie, social media services, relevant electronic services and designated internet services). However, that would appear to have the effect of extending this form of content regulation to services such as personal email (relevant electronic services) as well as to social media and potentially other services the Minister specifies.
- On the information provided in the Discussion Paper, it appears that in addition to the schemes applying to cyberbullying and image-based abuse (which have their own take-down regimes), there will be two categories of regulated content:
    1. 'Seriously harmful material', comprising child sexual abuse material, abhorrent violent material, and content that promotes, incites or instructs in serious crime, plus any additional types of content as determined by the Minister ('Class 1 content'). The services covered by these arrangements are the three categories in the EOSA (social media services, designated internet services and relevant electronic services). The scheme comprises statutory regulation, directly enforced by the eSafety Commissioner who 'classifies' the material with reference to the statutory category of 'seriously harmful material' and associated definitions. The eSafety Commissioner may issue take-down notices on the basis of this decision on the nature of the content.
    2. Prohibited or potentially prohibited content, comprising: RC or X18+ content; R18+ content that is not subject to aged-based restrictions; or MA15+ content not subject to aged-based access restrictions that is provided via a commercial content service or a mobile premium service ('Class 2 content'). It is simply not clear from the Discussion Paper whether the scheme would continue to apply, in large part, to websites and mobile premium services (as is the case for Schedules 5 and 7), or whether the three categories of service provider under the EOSA would apply here. Regulation will, in the first instance, be via codes of practice, though it is not clear whether consumers could complain directly to the eSafety Commissioner who would be able to issue take-down notices without the need for some intervening step, as is the case for code breaches under the BSA and the TA (see our comments on co-regulation in section 7 below). If codes fail or are not developed, the eSafety Commissioner can develop a standard.

- The ambiguities noted in point 2 above need to be addressed. The reference on p 43 of the Discussion Paper to a 'harmonised set of obligations for the take-down of seriously harmful content across the four schemes (cyberbullying, cyber abuse, image-based abuse and online content)' suggests the online content scheme may apply to all three categories of service under the EOSA. This reading is consistent with observations in the *Report of the Statutory Review of the Enhancing Online Safety Act 2015 and the Review of Schedules 5 and 7 to the Broadcasting Services Act 1992 (Online Content Scheme)*, noted above, but there is no explanation in the Discussion Paper as to why or how the online content scheme (which includes regulation of MA15+ and R18+ content) should apply to, say, social media or email. While we understand the appeal of regulatory consistency (including the benefits that would come from the separate compliance pathways for 'hosting services', 'live content services' and 'links services') its cost could be a serious erosion of freedom of expression. Accordingly, we oppose this sort of expansion of the online content scheme.
- Similarly, there is no explanation of how the overlap between RC material, which currently includes the types of material to be designated 'seriously harmful content', will be handled. It appears there is also a potential for overlap in the treatment of abhorrent violent material under the Criminal Code, which is also a form of seriously harmful content under the Online Safety Act.
- While we support the proposal for the eSafety Commissioner to make timely decisions on seriously harmful content, avoiding the delays involved in seeking classification by the Classification Board, we think there should be provision for review by the Classification Board of the eSafety Commissioner's decision. It is important to note here the difference between the decision in relation to the content and the decision to issue a notice. Under s 88 of the EOSA, a decision under s 35 to issue a take-down notice is reviewable by the Administrative Appeals Tribunal (AAT) (as is the decision not to issue a notice). We would expect this to be a part of the arrangements for 'serious harmful content', but in addition, there should be a mechanism for reviewing the characterisation of the content as 'seriously harmful content'. It would be appropriate for this to be done on application to the Classification Board (without limiting standing to the service provider and a person who is the subject of the content). We think this approach would be workable because 'seriously harmful content' is effectively a subset of RC content; and the new 'classification' and decision making mechanism are being developed to enable more effective regulatory responses, rather than to remove the classification of content by reference to community standards. This approach effectively retains the primacy of the National Classification Code and enforces a greater degree of transparency and accountability upon the office of the eSafety Commissioner. Irrespective of the decision maker, the National Classification Code underpins decisions in this country on community standards. It represents agreement among all Australian states and territories as to the basis for these content decisions. While it is reasonable to reform the cumbersome referral process for online content classification decisions, it is not acceptable to suggest merely that the eSafety Commissioner 'may' have reference to the Code.
- On a related aspect, we note that in their submission to the current Review of Australian Classification Regulation, researchers from Queensland University of Technology (led by Professor Terry Flew, who in 2012 conducted the Australian Law Reform Commission review, Classification: Content Regulation and Convergent Media) have proposed changing the category 'RC' to 'Prohibited'. This classification would capture content that is the subject of a criminal offence under relevant Acts. We support this approach.
- We do not support the proposal to give the Minister the power to specify new categories of 'seriously harmful material'. The examples given in the Discussion Paper of virtual reality and animated content describe media forms or formats, not types of harmful material.

7. Use of co-regulation

Questions 19 to 23 (p 40)

It appears from the discussion on pp 40-41 of the Discussion Paper concerning the proposed changes to the online content scheme that greater use will be made of co-regulation. There is to be a 'stepped process' of complaints to the service provider with escalation to the eSafety Commissioner. However, the Discussion Paper does not specify whether these arrangements would replace those in Schedule 7, under which consumers can complain directly to the regulator about breaches of the BSA, despite the co-existence of rules and complaint handling procedures in the codes of practice. It appears that most rules will be in codes or even subordinate instruments that give effect to general principles. These arrangements would only apply to 'Class 2 content' (the existing categories of RC, X18+, R18+ and MA15+), with material considered 'seriously harmful content' remaining with the eSafety Commissioner.

In our view, co-regulation and even self-regulation can provide effective and efficient ways of promoting positive obligations and of discouraging undesirable conduct. However, to be both effective and efficient, co-regulatory schemes must be well designed, implemented and administered. Our comments below are offered with this in mind.

- We agree that reviewing and where necessary updating and consolidating the codes developed under Schedules 5 and 7, now administered by the Communications Alliance, is appropriate in the context of updated legislation.
- While we acknowledge that current codes do not accurately capture the range of online services Australians now use, we have concerns about the proposal to extend the code provisions to 'a wider range of service providers … reflecting the range of online services Australians now use to access online content'. The online content scheme was developed principally for website content and also applies to mobile premium services and commercial content. Any proposal to extend it needs to indicate what type of services will be covered and why the extension is justified. As noted in section 2 above, we see no reason to apply the online content scheme in its entirety to comments posted by users on social media services such as Facebook and Twitter.
- We agree with the statement that it is appropriate that different sections of the industry/providers develop their own codes. We agree that the obligations on ISPs should be different to those on content providers, and we would extend this to digital platforms insofar as they should not be regarded as having the same obligations as content providers.
- Subject to seeing the drafting of these provisions, we support the principles-based approach to code formation, provided the codes remain enforceable. However, principles-based co-regulation would ideally be linked to outcomes that are set out in the legislation that creates the co-regulatory arrangements. If it is not intended that outcomes be specified in the legislation, we suggest that the eSafety Commissioner be given a power to specify outcomes in a determination. We assume operational aspects (eg, how providers seek to achieve the specified principles and outcomes) are to be dealt with in voluntary guidelines, but this is not explained. Finally, there also needs to be some consideration of matters where rules, not principles, may be required, as enforcement of principles can be difficult.
- We assume that 'approval by the eSafety Commissioner' means that the codes would be registered under the Online Safety Act. As there are important differences between the existing schemes in the TA and the BSA, such as the criteria for registration, further information is needed on any preferred approach. In any event, we strongly believe the registration criteria in s 123 of the BSA and s 117 of the TA should be improved upon for any new code registration scheme.
- One element of code registration involves the level of consumer and public consultation. There is no mention in the Discussion Paper of this element (other than the statement 'the codes would be developed in consultation with stakeholders'), even though the services being considered have been widely adopted by consumers. The BSA and TA have different

tests for the regulator to assess the adequacy of engagement when deciding to register a code: s 123(4)(b)(iii) of the BSA requires that 'members of the public have been given an adequate opportunity to comment on the code'; whereas ss 117(1)(f) and 117(1)(i) of the TA require, respectively, that members of the public be invited to make submissions within a specified period (ie, not less than 30 days) and 'at least one body or association that represents the interests of consumers has been consulted about the development of the code'. However, Lee and Wilding in *Responsive Engagement: Involving Consumers and Citizens in Communications Industry Rule-making* (November 2019, pp.89-91) note that the differences between the consultation provisions in the various statutory frameworks regulating the development of industry codes cannot be justified.

- We are concerned by the statement that 'the concept of harmful content under the codes would be informed by the National Classification Code …' (p 40). In our view, these codes should be based on, not informed by, the National Classification Code, and should go no further. This is an important aspect of protecting freedom of expression and access to content.
- In terms of enforcement, it is unclear what is meant by the comment that breaches of code provisions on RC or X18+ material would be 'treated very seriously'. The enforcement options for breach of a broadcasting code provision under the BSA are very weak, as no direct action can be taken in the first instance, even in the most serious cases. The ACMA has only two regulatory responses to a breach of a code of practice. First, it can accept an enforceable undertaking under s 205W, a subsequent breach of which would enable the ACMA to seek an order from the Federal Court to comply with the undertaking or pay an amount determined by the Court. An enforceable undertaking can provide for targeted and responsive enforcement, but the ACMA is only able to act if the broadcaster is prepared to provide the undertaking on terms acceptable to the ACMA. Second, in circumstances where the ACMA and the broadcaster cannot reach agreement, the ACMA's only regulatory enforcement action is an additional licence condition imposed under s 43. This is an even less satisfactory option as the only action the ACMA can take in response to a subsequent breach of this type of licence condition is the giving of a remedial direction under s 141. Regardless of the gravity of the breach, a penalty can only be sought from the Federal Court if the remedial direction itself is breached, following breach of the code of practice and then of the s 43 licence condition.
- In contrast to the code enforcement powers, in the case of a commercial television broadcaster, the ACMA can respond to a breach of a standard by various means. This is because under cl 7(1)(b) of Schedule 2 to the Act, breach of a standard comprises breach of a licence condition, which attracts the range of enforcement actions. In this case, the ACMA can: issue a remedial direction (s 141); accept an enforceable undertaking (s 205W); seek a civil penalty order from the Federal Court (s 140A); seek prosecution as an offence (s 139); or suspend or cancel the licence (s 143).
- The enforcement arrangements for broadcasting codes of practice are cumbersome and ineffective and should never be copied. Similar weaknesses appear in other legislative frameworks regulating the communications sector and merit further detailed review in order to better inform how enforcement provisions in the proposed Online Safety Act should be drafted.
- Despite the introduction of regulatory tools such as enforceable undertakings in the legislative amendments of 2006 to the BSA, the ACMA and commentators have argued for mid-tier powers to provide additional flexibility and responsiveness. In developing such options for the eSafety Commissioner under the Online Safety Act, the Department could consider similar reform to the BSA.
- For the co-regulatory arrangements to be effective, the regulator must have a power to initiate complaints (similar to s 173 of the BSA).

8. Governance and resourcing

Questions 36 to 39.

We note the options presented in the Discussion Paper for regulatory oversight of the Online Safety Act and the compliance and enforcement action that would be available to be taken under it. The options presented include enhancing the institutional independence of the office of the eSafety Commissioner or, alternatively, expanding the powers of the commissioner while transferring the institutional arrangements to the ACMA.

We recognise that governments are usually in the best position to assess such institutional arrangements and should have the authority to proceed with a scheme they feel will most effectively serve the legislative objectives. We have given careful consideration to this matter, taking into account the recommendations in the Briggs Report, and offer the following comments.

- On balance, we feel the functions of the eSafety Commissioner are likely to be best performed under the institutional arrangements of the ACMA. The ACMA should remain the accountable authority under the PGPA Act.
- The position of eSafety Commissioner should of course be maintained, given its success in dealing with specific issues and the opportunity it presents to target new regulatory efforts. But while the eSafety Commissioner has distinct functions, these operate within the broader context of the communications industry and regulation, meaning the community's interests are likely to be served most effectively through the access and close connection with the ACMA's other activities and in the exposure to 'board' level decision making offered by the presence of other Authority members. Moreover, completely separating the regulation of online content from the ACMA may pre-empt decisions to be made in the broader review of broadcasting regulation signalled by the Government in its response to the Final Report of the ACCC's Digital Platforms Inquiry.
- In addition to the benefits accruing in respect of governance and performance of statutory duties, there are clearly resourcing implications in establishing a new, fully independent entity. These will add to the costs of extending the cyberbullying protections to adults. As well as the costs savings from shared corporate functions, work in the areas overseen by the eSafety Commissioner, like that of the ACMA, is likely subject to ebb and flow; a larger organisation is better placed to deploy teams from one work area to another according to demand.
- In summary, we support Option 2 on p 57 of the Discussion Paper; we think the office of the eSafety Commissioner should be permanently merged with the ACMA (not a government department), with the eSafety Commissioner continuing to be an independent statutory office holder supported by ACMA staff as well as being an Authority member of the ACMA. This would promote internal transparency, more rigorous and accountable decision making, and explicit co-operation on related activities (eg, the administration of the online gambling advertising scheme in Schedule 8 of the BSA and the codes to be developed on disinformation). The existing arrangements under which ACMA and ACCC associate members join meetings of their governing bodies would also promote cooperation in relation to the schemes administered by the ACCC which address conduct by the same entities. Consideration could be given to the ways in which the Australian Human Rights Commission is established under the *Australian Human Rights Commission Act 1986* and operates under the PGPA Act with designated commissioners also exercising powers under other Acts. For example, the Sex Discrimination Commissioner has functions under the *Fair Work Act 2009*.