COMMUNICATIONS ALLIANCE LTD
www.commsalliance.com.au

AMTA
Australian Mobile
Telecommunications
Association

Submission
to the
Department of Communications and the Arts

Reviews of the *Enhancing Online Safety Act 2015* and the Online Content Scheme – discussion paper

Joint submission by:
Communications Alliance
Australian Mobile Telecommunications Association (AMTA)

25 July 2018

Background

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

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

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

The **Australian Mobile Telecommunications Association (AMTA)** is the peak industry body representing Australia's mobile telecommunications industry. Its mission is to promote an environmentally, socially and economically responsible, successful and sustainable mobile telecommunications industry in Australia, with members including the mobile carriage service providers, handset manufacturers, network equipment suppliers, retail outlets and other suppliers to the industry. For more details about AMTA visit http://www.amta.org.au.

Communications Alliance and AMTA (Associations) appreciate the opportunity to provide feedback on the *Reviews of the Enhancing Online Safety Act 2015 and the Online Content Scheme discussion paper* (discussion paper) released for consultation by the Department of Communications and the Arts.

Industry welcomes the review of the Online Content Scheme (OCS), which includes the above codes, and agrees that it is useful to consider the OCS in conjunction with the statutory review of the enabling legislation of the Office of the eSafety Commissioner (Office). As will be argued below, Industry also strongly recommends a review of the obligations contained in Schedules 5 and 7 of the *Broadcasting Services Act 1992* (BSA).

Introduction

The lives of those in the Australian community are increasingly influenced by an online environment in which they actively or passively participate. Access to the internet is widespread and is increasingly considered to be a basic human right. The internet has not only become an essential tool for formal and informal education in all areas of society but is also a key mechanism for communication and engagement. With one of the highest smart-phone penetration rates in the world and fast and reliable mobile internet in most of the populated areas of Australia, this online environment is now near-universally available at our fingertips 24/7.

Australian governments have created rules, guidelines and behavioural expectations on how to keep individuals safe in our physical environments (e.g. maritime, national parks, etc.) while simultaneously enjoying these physical environments and ensuring that the ecosystem of this environment can remain intact and flourish. Much in the same way, our society must create and apply certain standards for our online environment to ensure the safety of its citizens living in an online environment while providing fertile grounds for this environment to continue to evolve and to provide the online services that we have come to love and depend on.

The telecommunications industry, including internet service providers (ISPs), recognise that access to some online content, particularly by minors or vulnerable adults, may have detrimental effects on the physical, social and emotional well-being of the user and may also influence their values with regards to sexuality, relationships, violence, security, racial and religious equality and tolerance and many other key societal values. The proliferation of online social networking poses additional challenges around cyberbullying and the sharing of (sometimes intimate) images.

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

As described in the discussion paper, Australia has existing mechanisms and tools in place within both Government and Industry, including the Office of the eSafety Commissioner, to address many of the issues described above. As in the past, our industry continues to engage closely with all stakeholders, including enforcement agencies, and is keen to assist, where possible, to create and promote a safe online environment.

This submission will primarily provide feedback on the proposed review of the OCS and only address the review of the *Enhancing Online Safety Act 2015* (Online Safety Act) to the extent this relates to the effective functioning of the OCS.

Comments and Observations

Work and function of the Office of the eSafety Commissioner

The Associations commend the Office of the eSafety Commissioner on the work it has done in the past years. The Office has created a large number of useful resources and online information, education tools and programs for individuals, parents, families and schools. The Office also provides effective stakeholder engagement through the Online Safety Consultative Working Group, of which Communications Alliance, AMTA and other key industry players are active members.

The Office appears to be dealing effectively with complaints that it receives about illegal online content and associated take-down requests, and administers an efficient complaint system regarding cyberbullying material. The number of serious cyberbullying complaints resolved (830 complaints in the past three years[1]) suggests that many social media platforms operate very effective reporting tools and handle complaints directly addressed to them by users effectively. Consequently, there may be a reasonable degree of duplication in the schemes operated by the Office and Industry.

Following the broadening of the mandate of the Office to cover all of the Australian community (i.e. not only children), it appears that the role given to the Office of the eSafety Commissioner is appropriate, well-defined and backed by appropriate powers to effectively execute the functions assigned to the Office. Additional powers do not appear necessary at this point and only ought to be considered where clear evidence suggests that other approaches, including self and co-regulatory approaches, have not been able to deliver the desired outcomes and where an expansion of the mandate of the Office is a proportionate response to the identified risk.

The Office, being an independent statutory office, is well placed within the broader communications and media remit of the Australian Communications and Media Authority (ACMA). Industry does not see merit in the creation of a separate entity as defined in the *Public Governance and Accountability Act 2013*. Equally, at this stage, Industry does not see any reason to reduce the functions currently placed on the Office of the eSafety Commissioner.

Consolidation and review of underpinning legislation and regulation

As noted above, the current legislative and self/co-regulatory framework underpinning the OCS would benefit significantly from consolidation and a substantial review of its content in light of the technological developments of the past two decades and the advancements that are likely to occur in the (relatively near) future, such as the deployment of 5G, the burgeoning influence of the Internet of Things, progress in relation to virtual and augmented reality and the creation and widespread use of artificial intelligence.

Given Schedules 5 and 7 of the BSA already confer functions to the Office of the eSafety Commissioner, it would be more logical and efficient to consolidate those functions and other already existing functions in the Online Safety Act.

This process of consolidation ought to be accompanied by a thorough review of Schedules 5 and 7 which, so we anticipate, ought to result in the creation of one single 'schedule' relating to online services and content under the Online Safety Act.

As the discussion paper indicates, Schedules 5 and 7 of the BSA date from 1999 and 2007. Industry regards the two schedules as generally outdated or misaligned with today's technologies and usage of online technologies. The two schedules lead to inconsistent treatment and access requirements of the same content across different platforms, thereby

[1] p.13, Reviews of the Enhancing *Online Safety Act 2015* and the Online Content Scheme – discussion paper, Department of Communications and the Arts

creating customer confusion and a complex and unnecessary regulatory burden for Industry. Consequently, the two schedules must be reviewed, with a view to creating a technology and delivery platform-neutral approach.

It should also be noted that the OCS regulates services which are not broadcasting services. Given that the Online Safety Act provides a clear alternative that is dedicated to the specific subject matter of online safety, it appears more efficient to move the OCS into this legislative framework.

As Schedules 5 and 7 form the basis for the existence and much of the content of the Internet and Mobile Content Codes and the *Content Services Code*, these Codes have not been able to be revised for almost a decade and, consequently, are difficult to comply with for industry.

More importantly, the constraints imposed by the BSA onto the adaptability of the OCS have resulted in a misalignment of legislation and technological realities – a radically changed online environment and evolved community expectations. As a result, the OCS, much like the BSA, provides inconsistent treatment of the same content across different platforms. The current OCS also does not reflect the current high levels of mobile phone usage by children (and the broader Australian community) and the way we all access and consume online content, especially via social media platforms as opposed to traditional internet/mobile content models.

Since its inception, the OCS has also seen a migration of illegal content from domestic websites to websites hosted offshore, which means that the earlier focus on take-down notices is now less efficacious and valuable. Overall, it seems that the current OCS should be rebalanced to address concerns raised about minors accessing illegal content hosted offshore and could be enhanced to provide better safeguards for the community.

The Associations contend that the co-regulatory approach of the OCS is working and remains the most effective and efficient approach to online safety. Therefore, industry recommends retaining the ability for an industry body representing the internet industry to develop industry codes under the Online Safety Act while maintaining the Commissioner's reserve powers to make an industry standard if the co-regulatory regime is proven ineffective.

Given the dynamic and fast-changing nature of the environment in which any legal or regulatory instrument needs to operate, it appears that industry codes are more suitable to more flexibly address changes in technology and community expectations than 'black letter law', which can be cumbersome to amend in the timeframes required. Importantly, it ought to be noted that there is no evidence to suggest that an alternative approach will deliver better protections for end-users.

It is key to highlight that Industry's ability to update codes to align with future technologies and changing community expectations relies on less prescriptiveness in the underlying legislation. The current codes that form part of the OCS are outdated and have not been revised due to the prescriptive nature of Schedules 5 and 7 of the BSA which prevented a meaningful overhaul of the codes. It is, therefore, of utmost importance to ensure that any revised underlying legislation, such as a proposed single 'schedule' within the Online Safety Act, is sufficiently principles-based and flexible to allow future adjustments to the industry codes of the OSC.

In summary, Industry recommends the consolidation of Schedules 5 and 7 into a single piece of legislation that ought to be contained within the Online Safety Act. Furthermore, as the owner of the industry codes that form part of the OCS, the Associations advocate for the development of a single, technology and platform neutral industry code that is enforceable by the Commissioner.

Our industry is ready to engage with all relevant stakeholders over the development of an industry code that replaces the existing industry codes within the OCS.

Classification of content

Industry believes that content ought to be classified under a classification scheme, and it appears that the current National Classification Scheme suits that purpose. However, for any classification and potentially resultant take-down notices to have the desired effect of protecting end-users (and especially vulnerable users, e.g. children) and victims and preventing the re-victimisation through prolonged exposure of content that ought to be taken down quickly, it is imperative that the classification of content can occur within very short timeframes.

From Industry's perspective, it is of lesser importance which organisation is undertaking the classification, so long as the classification occurs correctly and within very short timeframes. It appears that this is currently not the case, with classification timeframes of up to 30 days.

We note Government has also planned a review of the classification regime. It is critical that any action taken as a result of this review does not create the risk of inconsistencies for classification of the same content. Therefore, any classifying organisations (should there be more than one) ought to undergo the same training and classify content across all platforms consistently and by the same guidelines.

Family Friendly Filter Scheme

In general terms, filters are computer programs designed to limit access to certain types of content on the internet. Such filters operate in different ways, and different filters will be better suited to different operating environments and age groups.

The use of filters by end-users is not mandatory in Australia, neither under law nor the existing industry codes. Users can choose whether or not to install filters, and if and when to activate them. Likewise, ISPs are not required to filter or monitor internet traffic.

However, under the relevant industry codes all ISPs in Australia are required to promote to their customers an accredited internet content filter under the FFF Scheme, and if the customer can purchase it directly from the ISP, it must be provided at or below cost price. To qualify for FFF status, a filter must undergo rigorous independent testing to ensure that it meets the criteria as set out in the relevant industry code. These include effectiveness, ease of use, configurability, availability of support and agreement by the company providing the filter to update the filter as required by the Office, for example where the Office determines following a complaint, that a specified site is prohibited under Australian law.

A revised and consolidated industry code as proposed above could further be enhanced by a revived FFF Scheme and accompanied by various complementary initiatives that the telecommunications industry already has in place and will continue to evolve to improve the online safety of the Australian community.

In addition to the FFF Scheme, it is important to note there are a number of other end-user-based internet filter programs are available, either commercially from third parties or as part of the services offered by ISPs to allow users to control access to internet content by children. These filters are not necessarily less effective.

ISP-based filtering

The Associations caution against the re-opening of the debate around ISP-based filtering or blocking of websites in the context of the review of the OCS. The blocking of websites through ISPs – or mandatory ISP-based internet filtering schemes as previously proposed (and withdrawn) in political debate – are regularly considered by those outside the industry as a solution to issues associated with the access to undesired and illegal content or activities on the internet. In this context, it is important to understand that there are far more effective tools and resources available that carry less risk of negative side effects and provide users and guardians with a greater degree of control.

Industry recognises that website blocking (the blocking of websites at an ISP level) has a legitimate place in law enforcement and, accordingly, under Section 313 of the *Telecommunications Act 1997*, the Australian telecommunications industry is assisting law enforcement agencies with the blocking of sites in the context of specific illegal content.

However, website blocking is a relatively blunt tool and has the potential for comparatively easy evasion (through the use of VPNs, use of the Tor network or Tor and other browsers, anonymous proxies, HTTPS access, SSH tunnels, remote desktop clients and purpose-built programs). Website blocking carries with it the potential to over-block, hamper legitimate activities and disadvantage consumers. It also has the potential to extend outside original intentions, e.g. it may capture websites and content that were not intended to be targeted by the blocking.

Even where such blocks are correctly targeted, they only provide a partial solution to the problem, due to the large volume of ISPs (more than 400) in Australia and the complexity of successfully requesting all ISPs to install a block.

Most importantly, filtering and blocking of websites at an ISP level will equally deny access to these websites of anyone who wishes to access them (and is legally allowed to do so), i.e. a differentiation of who should be able to see what sort of content on the internet is not possible.

Given the risks and infringements of personal rights and freedoms associated with website blocking, the high costs involved with the execution of site blocking (it requires highly trained technical staff), the ease with which it can be circumvented and given that there are alternative means which equally or more effectively achieve the objective of protecting users from potentially harmful content, the ISP-based blocking of websites must be considered as not meeting any proportionality test and ought to be discarded in the discussion around online safety.

Industry measures around online safety and digital education

In addition to the FFF Scheme and commercial end-user-based filters, Industry (as well as many other Government and non-government organisations) offers a suite of tools and resources to educate the community about the risks of using the internet and to enable the Australian community to manage their use of the internet within boundaries that they may wish to set. Some examples include:

- iiNet: https://www.iinet.net.au/about/community/learn/cyber-safety/
- Optus: https://www.optus.com.au/about/sustainability/responsibility/cyber-safety
- Telstra: https://www.telstra.com.au/consumer-advice/cyber-safety
- TPG: https://www.tpg.com.au/about/online_safety.php
- VHA: https://www.vodafone.com.au/about/sustainability/digital-parenting
- Google: https://www.google.com.au/safetycenter/
- YouTube: https://www.youtube.com/yt/policyandsafety/safety.html

Many over-the-top providers of social networking and communications services expressly prohibit the distribution of sexually explicit/pornographic, overly violent etc. materials on their platforms (for example, Google's *User Content and Conduct Policy*[2], the YouTube *Community Guidelines*[3] and Facebook's *Community Standards*[4]).

Platforms such as YouTube, Google Search, and iTunes also offer 'safe modes' or the ability to enable restrictions to allow parents to control purchases and/or restrict inappropriate content from appearing within search results.

[2] https://www.google.com/intl/en-US/+/policy/content.html
[3] https://www.youtube.com/yt/policyandsafety/communityguidelines.html
[4] https://www.facebook.com/communitystandards

As previously mentioned, Industry also cooperates very closely with relevant enforcement authorities to combat the availability of child sexual abuse material on the internet, including through the blocking of websites on the INTERPOL 'worst of' list[5] under law (i.e. Section 313 of the *Telecommunications Act 1997*).

In addition, many ISPs and content providers/platform operators offer a suite of educational programs that specifically target digital education and online safety of individual groups, such as senior citizens, women or indigenous users.

Industry players also have co-founded and/or lend their ongoing support to educational efforts by third parties and programs, such as ReachOut, The Alannah and Madeline Foundation, Kids Helpline, Project Rockit, Bravehearts, eSmart Libraries, eSmart Digital Licence and the eSmart Schools Program to mention a few, to actively support efforts to raise awareness and educate young people about digital citizenship.

Broader educational approaches to online safety

It is critical that the (warmly welcomed) review of the Online Safety Act and the OCS do not distract from the fact that a wider, well-structured and educational framework – harmonised at a State and Federal level – ought to be at the centre of the debate on how to address issues surrounding online safety.

It is also important to recognise that many of the public policy issues that are being debated in the online context also exist in the 'offline world'. We must avoid singling out the online context for attention at the expense of considering complex issues more holistically as broader societal challenges.

Industry recognises the creation of the Office of the eSafety Commissioner as a key measure to a coordinated national approach and we commend the Office on its good work so far. However, an overarching framework combining cyber security and online safety ought to consider how the Australian community's exposure to potentially harmful content and their involvement in potentially detrimental online activity (e.g. as a result of overly generous sharing of private information, cyberbullying or identity theft) can be minimised without undue limitation of citizens' rights and freedoms. This ought to include educating end-users about user-based filters and apps to manage online behaviour.

The discussion paper raised the questions whether the OCS is effective in limiting the availability of prohibited content and whether it is providing adequate safeguards for children. It should be noted that no existing, revised or new legal, regulatory and technical mechanisms will be able to completely safeguard the Australian community from harm that may arise from their online environment. Therefore, it is paramount to teach the community, especially children, appropriate online behaviour, cultivate resilience and encourage end-users to report illegal and concerning activities and content to authorities if need be. This ranges from issues such as the disclosure of personal information, posting explicit photos, cyberbullying etc. to content that users consume which may have detrimental effects on their physical, social and emotional wellbeing.

Importantly, any 'online safety/behaviour education' must go hand-in-hand with a concerted effort by society in general to imprint the desired underlying values onto all citizens.

The Associations do not seek to comment in detail on educational measures, messages and their delivery, or on how to create an overarching online safety framework as others will be better placed to comment on this aspect and much has already been achieved through the Office of the eSafety Commissioner. Also, further research may be required to adequately address societal issues in a coordinated manner.

[5] Details can be found here: http://www.interpol.int/Crime-areas/Crimes-against-children/Access-blocking

Conclusion

The Associations look forward to further engaging with Government and other organisations on the mutual desire to ensure that the Australian community is well-equipped to safely enjoy online environments.

We believe that they current co-regulatory approach is appropriate but consider that the OCS and Schedules 5 and 7 of the BSA will benefit from a thorough review. Consequently, our industry stands ready to develop a more technology and platform-neutral industry code that better reflects today's online environment and community expectations.

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