COMMUNICATIONS ALLIANCE LTD

COMMUNICATIONS ALLIANCE

Submission to the

Senate Standing Committees on Environment and Communications Inquiry into

Harm being done to Australian children through access to pornography on the internet

March 2016

TABLE OF CONTENTS

INTRODUCTION		**3**
1.	**TERMS OF REFERENCE**	**4**
2.	**CURRENT FRAMEWORK**	**4**
3.	**POTENTIAL MEASURES**	**7**
4.	**CONCLUSION**	**11**

INTRODUCTION

Communications Alliance appreciates the opportunity to provide a submission in response to the Senate Standing Committees on Environment and Communications Inquiry into the *Harm being done to Australian children through access to pornography on the Internet*.

ABOUT COMMUNICATIONS ALLIANCE

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

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

1. Terms of Reference

The Terms of Reference of the inquiry are stated as follows:

"That the following matter be referred to the Environment and Communications References Committee for inquiry and report by the first sitting day in December 2016:

Harm being done to Australian children through access to pornography on the Internet, with particular reference to:

a. *trends of online consumption of pornography by children and their impact on the development of healthy and respectful relationships;*

b. *current methods taken towards harm minimisation in other jurisdictions, and the effectiveness of those methods;*

c. *the identification of any measures with the potential for implementation in Australia; and*

d. *any other related matters*."[1]

Communications Alliance does not seek to comment on the first two questions raised by the Terms of Reference (items a. and b.) but notes that a thorough analysis of the actual issue is required and, on an inquiry level, ought to precede any attempts to identify any measures with potential for implementation (item c.).

It is particularly important to view the potential harm being done to children by online pornography in context with other social issues, such as the consumption of illegal substances and alcohol, domestic and other violence, religious or racial intolerance etc., which are also very likely to be significantly affected by the consumption of content on the internet, prior to the identification of (perceived or real) measures for implementation in Australia.

As it stands today, Australia already suffers from a fragmented approach to cyber security and online safety and the lack of an overarching cyber security and online safety framework which could take into account the wider societal issues mentioned above.[2] Any further piecemeal approach to regulation and legislation ought to be avoided to limit overall inefficiencies, potentially sub-optimal policies and regulations as well as practical difficulties.

Communications Alliance notes that the Cyber Security Review Report was due to be released in November 2015. Unfortunately, Industry has not received any formal information as to when it can expect publication of the report.

2. Current Framework

Industry recognises that unlimited access to pornography by children[3], be it online or through other media, may have detrimental effects on their physical, social and emotional wellbeing and influence their values with regards to sexuality and relationships. Consequently, Industry appreciates that access to pornography via the internet may be harmful to children and that parents ought to be able to limit the exposure of their children to such content. Equally, society at large has a responsibility to ensure that children are educated and well equipped to become ethical and responsible online citizens.

[1] See, http://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Environment_and_Communications/Online_access_to_porn/Terms_of_Reference

[2] For further commentary on Australia's cyber security landscape and approach, refer to the Communications Alliance submission to the Department of the Prime Minister and Cabinet Consultation Paper *Cyber Security Review*, http://www.commsalliance.com.au/__data/assets/pdf_file/0009/48519/150402_CA-submission-PMC-Cyber-Security-Review_FINAL.pdf

[3] For the purpose of this submission 'children' shall refer to persons under the age of 18 years.

Industry (as well as many other Government and non-government organisations) offers a suite of tools to the community to educate parents, educators and children about the risks of using the internet and to enable them to manage children's use of the internet within boundaries that they may wish to set. Some examples include:

- iiNet: http://www.iinet.net.au/safety
- Optus: http://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: http://www.vodafone.com.au/aboutvodafone/corporateresponsibility/support-for-parents
- Google: www.google.com.au/SafetyCentre
- The Office of the Children's eSafety Commissioner: https://www.esafety.gov.au/education-resources

Many over-the-top providers of social networking and communications services expressly prohibit the distribution of sexually explicit and pornographic materials on their platforms (for example, Google's *User Content and Conduct Policy*[4], the YouTube *Community Guidelines*[5] and Facebook's *Community Standards*[6]). Industry also cooperates very closely with relevant 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[7]. (Note that the content on that list is illegal, and is blocked via a law enforcement request under the *Telecommunications Act 1997* (Act).)

However, it is important to note that pornography (i.e. legal content) is also being accessed legally and by deliberate choice by millions of Australian adults. Any measures to protect children from harm through access to online pornography must be balanced with the rights of adults to freely access such content, as well as the effectiveness and efficiency of measures that may be designed to limit children's online access to pornography.

Current regime

It is helpful to understand the basics of the regulation surrounding online content when discussing the issue of online pornography and the effects it may have on children. The following provides a rough overview of the principles of the current regime. It is not designed to give a comprehensive overview of what is a rather complex legal framework.

Illegal Content

The Australian Classification Board makes classification decisions about films, computer games and publications under the *Classification (Publications, Films and Computer Games) Act 1995 (Classification Act)* and the *Broadcasting Services Act 1992* (BSA) for internet content.

Australian providers are prohibited from hosting content within Australia that is classified R18+ (unless subject to a restricted access system), X18+ or RC[8]. Hosting as well as accessing child sexual abuse material is illegal under all circumstances and is actively monitored by authorities.

The recently created Office of the Children's eSafety Commissioner[9] (Office) is "responsible for leading online safety education for Australian children and young people, protecting

[4] https://www.google.com/intl/en-US/+/policy/content.html
[5] https://www.youtube.com/yt/policyandsafety/communityguidelines.html
[6] https://www.facebook.com/communitystandards
[7] Details can be found here: http://www.interpol.int/Crime-areas/Crimes-against-children/Access-blocking
[8] Restricted (X18+) films are restricted to adults. This classification is a special and legally restricted category which contains only sexually explicit content. That is, material which shows actual sexual intercourse and other sexual activity between consenting adults. Refused Classification (RC)is banned content.
[9] http://www.esafety.gov.au

them when they experience serious cyberbullying and managing complaints about offensive or illegal online content."[10]

Accordingly, the Office is responsible for receiving and investigating complaints under the BSA. Once it receives a complaint about online content, the Commissioner is required to make a determination as to whether the content is prohibited or likely to be prohibited. If it is, the below mechanisms apply.

The Office prioritises investigation of complaints about child sexual abuse material and other illegal online content, including sexual images and videos of Australian children. The Office also works with the international community of internet hotlines, known as INHOPE, to have overseas-hosted online child sexual abuse images taken down.

The same principles apply for overseas content. However, the enforcement mechanisms differ depending on whether the content is offered through an Australian provider or through an overseas provider: Australian content providers are subject to a take-down notice for prohibited content whereas content hosted overseas is referred to accredited providers of Family Friendly Filters[11] for inclusion on their blacklists in accordance with Internet Industry Association (now Communications Alliance) industry codes[12].

It is noteworthy that, in its first six months of operation, the Office has experienced considerable demand from the community for education resources and self-help information rather than regulation. The Office indicated that since 1 July 2015 it has had 1.44 million websites visits to its education resources and educated over 60,000 students, teachers and pre-service teachers face-to-face. Over 10,000 students across the Australia have also used the Cybersmart Virtual Classrooms to learn more about online safely.

Legal Content

Of course the internet also offers a range of legal content which millions of Australian adults (and children) choose to access but which may not always be appropriate for children.

A number of voluntary end-user based internet filter programs are available either commercially from third parties or as part of the services offered by Internet Service Providers (ISPs) to allow users to filter internet content. 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.

It is important to note that the *use* of filters by end-users is not mandatory in Australia, either under law or the 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 make available an accredited internet content filter (Family Friendly Filter) at or below cost price.

To qualify for Family Friendly Filter 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.

[10] See https://www.esafety.gov.au/about-the-office/role-of-the-office
[11] See http://www.commsalliance.com.au/Activities/ispi/fff
[12] The relevant codes in this context are the *Code for Industry Co-Regulation in Areas of Internet and Mobile Content* and the *Content Services Code*. For further information refer to http://www.commsalliance.com.au/Activities/ispi.

3. Potential Measures

Technical measures:

Website blocking

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 illegal, fraudulent or pornography related activities and content on the internet.

Industry recognises that website blocking has a legitimate place in law enforcement and, accordingly, under Section 313 of the Act, the Australian telecommunications industry is assisting law enforcement agencies with the blocking of sites which are classed as the 'worst of' (Interpol blacklist) and other illegal content.

However, website blocking is a relatively blunt tool and has the potential for comparatively easy evasion and to over-block, thereby capturing many other entities, including schools, universities, libraries and cloud-based services in ways that may hamper their legitimate activities and disadvantage consumers. Importantly, it has the potential to extend outside original intentions, e.g. it may capture websites and legitimate content that was not intended to be targeted by the blocking. (This was the case in the so-called ASIC-incident where the use of Section 313 of the Act to request blocking of a site also resulted in the inadvertent blocking of thousands of additional websites, refer to Sections 2.20 to 2.25 of the report "*Balancing Freedom and Protection*"[13] prepared by the House of Representatives Standing Committee on Infrastructure and Communications.)

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

Moreover, it should be noted that site blocking is easily overcome by users that wish to access a blocked website through the use of VPNs, use of the Tor network or Tor browser, anonymous proxies, HTTPS access, SSH tunnels, remote desktop clients and purpose built programs.

It can be also argued that the new data retention regime has made consumers more aware of the fact that their communication history is now captured and, consequently, more of these tools are coming into the market and are becoming popular in the mainstream community as everyday tools.

Means to circumvent website blocking

VPNs

VPNs encrypt the traffic between the user and the website so that the ISP is unable to determine the source or content of the traffic. VPNs have a legitimate place ensuring privacy and security of sensitive communications, and there are a range of commercial VPN providers, e.g. vyprVPN, purevpn, overplay, HideMyAss, ipvanish, CyberGhost etc. As the examples of Netflix and other online streaming providers prior to their official entry into the Australian market have demonstrated, current generations of children are well capable to install and use VPNs to circumvent blocking of websites and to access the content that they wish to consume.

[13] House of Representatives Standing Committee on Infrastructure and Communications, *Balancing Freedom and Protection*, issued 1 June 2015; see http://www.aph.gov.au/Parliamentary_Business/Committees/House/Infrastructure_and_Communications/Inquiry_into_the_use_of_section_313_of_the_Telecommunications_Act_to_disrupt_the_operation_of_illegal_online_services/Report

Tor

Once the domain of 'hacktivists' to access the deep web, the Tor network and Tor browser is now well known and in popular use by children and students to anonymously access websites. School content filters are regularly evaded using this method. It is easy to download the Tor browser to a computer or device and to connect to the Tor network. Once installed the browser is easy to use. Comprehensive deep packet inspection of all traffic would be required in order to render the Tor network and software ineffective in a blocking context. Such inspection practices in turn would be very likely to raise privacy concerns.

Anonymous proxies

Anonymous proxies enable users to access blocked websites and browse anonymously by tunnelling traffic over a regular or encrypted HTTP session. They are a popular choice with teenagers looking to bypass web filters. Detected proxies are being replaced almost immediately by one (or more) new proxies. Therefore, to effectively block anonymous proxies would require an ongoing real time solution with auto updates of known anonymous proxies. Such a solution, apart from being very costly, would be likely to add little benefit due to the 'cat and mouse' nature of the issue.

HTTPS access

HTTPS provides secured and encrypted connections thereby making it extremely difficult to determine whether the traffic under consideration is critical and related to a genuine activity, or whether a child is seeking to access a restricted website, and there is also no network-based solution that could do so. It is also not possible to completely (and uniquely) restrict access to HTTPS traffic.

SSH tunnels

SSH is a tool for securely accessing servers. However, it can also be used for tunnelling purposes. Tunnelling allows a user to forward a port on a remote server to one on a local server. This is especially useful for web developers because it allows creation of a tunnel between a local web server and the internet which allows anyone to access a local app or website. However, students or more sophisticated teenagers have been known to create SSH tunnels to access blocked content. Once an SSH connection has been established, traffic can be tunnelled through to an external SSH server to connect to another computer remotely in order to access any desired content and circumvent firewalls or web filters. Again, there is no network-based solution that would allow elimination or reduction of those practices.

Remote desktop clients

A number of remote desktop applications exist (e.g. GoToMyPC and Microsoft Remote Desktop) that facilitate access to another PC from anywhere. A child using this type of application can access another network that can evade a web filter.

Purpose built software to avoid content filters

There are a number of desktop proxy applications (e.g. Ultrasurf and Your Freedom) designed to allow users to bypass content filters, evade censorship and protect their online privacy. These applications are purpose-built to encrypt traffic to bypass filters by transforming the local device into a web proxy to connect directly to hosted proxies. These applications have many ways to avoid web filters such as tunnelling through firewalls, sending traffic via web proxies, FTP proxies, DNS servers and more. These applications are easily installed and many video tutorials, that walk users through the set-up process, are available online.

Blocking practicalities

Most importantly, blocking of websites at an ISP level will equally deny access to these websites to adults who legitimately wish to access them and are legally allowed to do so.

It also appears that it may be difficult to define the actual content displayed/offered on websites that were to be blocked, i.e. it may be very difficult to 'draw the line' between explicit (but not blocked) content and content considered to be of pornographic nature which, therefore, would be blocked.

In July 2013, the UK introduced an ISP-based website filtering scheme with all four major ISPs offering filtering of websites that are deemed obscene or dangerous. Subscribers must actively opt out if they do not wish the filter be applied. UK's regulator, Ofcom, found that subscribers overwhelmingly had opted-out of the filter with three of the four large ISPs only having less than 10% of their subscriber base using the filter.

Equally, research by Broadband Genie[14] amongst close to 2500 users showed that 41% believe that ISPs should not block pornographic websites by default. 54% had opted out of using filters and a further 22% were unsure (which may indicate that they were unlikely to attribute a significant importance to the existence of filters). Importantly, 40% of those opting out cited the risk of internet access being hindered as a key reason for not activating the filter. And indeed, of those who did opt to keep the filter activated, 51% had experienced a block of a seemingly legitimate website. Interestingly, 27% were concerned that authorities would be keeping a list of subscribers who opted out of using the filter. And overall 60% of respondents said that they were unsure whether network website filtering is effective or they even believed it mostly ineffective or totally useless.

Also, any website blocking or ISP-based internet filtering operating on the basis of 'blacklists' will be impractical as filtering lists will not be able to keep pace with the creation of new content or the resurgence of filtered content under slightly different domains, e.g. identical content moving from www.prographymaterial.com to www.pornografy.com (fictitious websites).

Moreover, this approach is fraught with danger of scope creep and a desire to expand the blocking to all sorts of other content that may be deemed inappropriate or undesirable. Issues that regularly come up for discussion in this context include, for example, content relating to hate speech or content with a likelihood to promoting eating disorders in children.

The Internet Architecture Board concluded in its recently published paper *Technical Considerations for Internet Service Blocking and Filtering* that "(…)there are no perfect or even good solutions -- there is only least bad (and a specific technical method) may prove least damaging".[15]

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 (discussed below) which equally or more effectively achieve the objective of protecting children from potentially harmful content, the ISP-based blocking of websites must be considered not meeting any proportionality test and ought to be discarded in the discussion around the protection of children from potentially harmful, but *legal*, content.

Voluntary user-based internet filters

As indicated above, there is a large range of internet filter programs with varying capabilities on the market. Internet filter software works by giving parents the ability to create specific user IDs for individual family members who use one (or several) devices thereby enabling parents to set restrictions based on age or maturity level. The filter software allows parents to block websites, filter content, receive alerts (e.g. if children are being cyber-bullied) and oversee all aspects of a family's online activities. Some of the filter programs can send real-time alerts to notify parents of the development of potentially dangerous situations.

[14] See https://www.broadbandgenie.co.uk/blog/20150804-isp-filter-survey
[15] https://tools.ietf.org/html/rfc7754

Most software will also include reporting features that provide summaries of all online activity, and some will allow alerts to users that their activity will be reported to parents if they proceed to access previously specified websites. A number of programs include the ability to capture screenshots, log chat conversations, and copy parents on inbound and outbound emails for potential review. Many now also have the ability to monitor social media platforms such as Facebook, Tumblr, Instagram, Twitter etc.

Internet filters typically either operate on a monthly subscription basis or a yearly licence which appears to cost in the range of $30 to $70 per year (with the more expensive filters not necessarily being the best performing).

Many of the internet filters available can be used on mobile devices such as tablets and smartphones, in addition to computers. Furthermore, internet filters are complemented by a plethora of specific parental control apps for mobile devices which are available for free or a charge from easily accessible sources, e.g. on the device itself, or via the AppStore or Google Play. There are also additional in-built controls in place on mobile devices that can be used to control children's use of the mobile device.

Industry is also working with Government to help Australians better access existing and new commercial parental control tools and filters and has formed the Child Online Safety Tool Working Group to consider a range of measures to make the optional use of parental control tools even easier for consumers.

It should be noted that platforms such as YouTube, Google, 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.

Voluntary user-based internet filters constitute a very powerful means to prevent children from accessing content that their parents deem unsuitable for them. Importantly, such content can then easily be extended to include other areas such as drug related content or violence. Conveniently, internet filter software can also be used to establish limits on how many hours children spend online.

Therefore, user-based internet filters, apps and software offered by ISPs and mobile operators constitute a cost efficient means to achieve highly targeted and effective protection from potentially harmful content on the internet (which goes beyond pornography) without bearing the same risks of inadvertent 'over-blocking' and denying other users the freedom to access content that they wish to consume.

Educational measures:

Industry, as many other organisations, contends that a wider, well-structured and educational framework – harmonised at a State and Federal level – must be at the centre of the debate on how to address issues surrounding the potential harm to children through online pornography as well as many other potentially harmful types of content that are legally available on the internet.

Industry recognises the creation of the Office of the Children's eSafety Commissioner as an important first measure to a coordinated national approach. However, an overarching framework combining cyber security and online safety ought to consider how children's exposure to potentially harmful content – beyond online pornography – and their involvement in potentially detrimental online activity (e.g. as a result of overly generous sharing of private information or identity theft) can be minimised (if minimisation is desired) without undue limitation of citizens' rights and freedoms. This could include educating parents about user-based filters and apps to manage children's online behaviour.

It should be noted that no amount of content control is likely to completely eliminate children's exposure to potentially harmful content. Therefore, it is much more important to teach children appropriate online behaviour and cultivate resilience so that if they do see something that concerns them they have the internal tools to process and consider what they have seen, and understand how they can report this to authorities if need be. This ranges from issues such as the disclosure of personal information, posting explicit photos,

cyber-bullying etc. to content that they consume which may have detrimental effects on their physical, social and emotional wellbeing.

It appears that there is already a vast amount of information available to parents, carers and educators. Notably, with the establishment of the Office of the Children's eSafety Commissioner, a national Government agency has already taken charge of at least some of the areas associated with online safety. Yet, a structured overarching approach to cyber security and online safety seems to be missing and is urgently required.

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, e.g. in the case of pornography, the value of women (and men as the case may be) as equal partners as opposed to 'sex objects', the value of healthy partnerships, consensual sex etc.

Communications Alliance does 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. Also further research may be required to adequately address societal issues in a coordinated manner.

4. Conclusion

Communications Alliance is happy to continue to engage with Government, Parliamentary Committees and other organisations on the mutual desire to ensure that Australian children are equipped to deal with a more digital society and the challenges that may come with it.

However, as evidenced in this submission, Industry believes that further regulation of the telecommunications industry, which is merely facilitating access to content, is neither an appropriate nor effective way of addressing the issues that the Australian society, and children in particular, may face.

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

COMMUNICATIONS
ALLIANCE LTD

Level 12
75 Miller Street
North Sydney
NSW 2060 Australia

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