COMMUNICATIONS
ALLIANCE LTD

# COMMUNICATIONS ALLIANCE

## Submission
## to the
## Department of Communications and the Arts
## Discussion Paper

## *Civil penalties regime for non-consensual sharing of intimate images*

June 2017

# TABLE OF CONTENTS

# INTRODUCTION

Communications Alliance appreciates the opportunity to provide a submission in response to the Department of Communications and the Arts (DoCA) Discussion Paper on a proposed *Civil penalties regime for non-consensual sharing of intimate images* (Discussion Paper).

## 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 and Wider Context

The Discussion Paper states that views are being sought on:

a) "how a proposed civil penalty regime might best complement existing regulation and other initiatives, and how it might be framed;
b) the expansion of the role of the Commissioner to administer the new scheme, and how the Commissioner might enforce the civil penalty regime; and
c) definitions of key terms and behaviours."

Communications Alliance does not seek to comment on items a) and c) but intends to confine its feedback to issues that ought to be considered if a civil penalties regime was to be implemented. Our commentary will centre around Recommendation 14 of the Discussion Paper:

| Should the Commissioner be able to seek a court order to require Internet Service Providers (ISPs) to block individual website(s) in extreme cases where all other avenues have been exhausted? |
|---|

In this context, we also will draw attention to issues that the telecommunications industry, as providers of the technical infrastructure that facilitates access to online content and the exchange of information, already encounters today.

Industry recognises that non-consensual sharing of intimate images can cause harm, distress, humiliation and embarrassment and, consequently, can severely (negatively) affect a victim's reputation, employment, family and relationships. In more extreme cases, it may also affect personal safety, either through actions from third parties or through self-harm and suicide.

It is important to view the issue of non-consensual sharing of intimate images and the potential harm caused by it in context with other societal issues, such as the potential harm being done to children through access to pornography on the internet, the use of the internet for online gambling or the infringement of copyright facilitated by the use of the internet and infringing bit-torrent sites etc.

Like many other societal issues relating to the use of modern technologies, combatting non-consensual sharing of intimate images is likely to require a multi-pronged approach with a key focus on education from various directions.

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

- iiNet: https://www.iinet.net.au/about/community/learn/cyber-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/about/sustainability
- Google: http://www.google.com.au/safetycenter/
- The Office of the eSafety Commissioner: https://www.esafety.gov.au/education-resources and https://esafety.gov.au/esafety-information

Many over-the-top providers of social networking and communications services expressly prohibit engagement in bullying and threatening behaviour and the sexualisation of persons

in an unwanted way on their platforms (for example, Google's *User Content and Conduct Policy*[1], the YouTube *Community Guidelines*[2] and Facebook's *Community Standards*[3]).

As it stands today, Australia already suffers from a fragmented approach to online safety and cyber security and the lack of an overarching online safety and cyber security framework which could take into account the wider societal issues mentioned above.[4] 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 recent initiatives around online safety and cyber security, e.g. the Prime Minister's Cyber Security Roundtable and any resulting initiatives, ought to align with the proposed new regime.

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

# 2. Background on Website Blocking

As Recommendation 14 of the Discussion Paper points to the potential use of website blocking, it may be useful to briefly summarise the current legal background and technical issues surrounding website blocking.

**Current legal background**

Industry recognises that website blocking has a legitimate place in law enforcement and, accordingly, under Section 313 of the *Telecommunications Act 1997* (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. Currently, Section 313(3) of the Act only applies to Carriers/Carriage Services Providers (C/CSPs) who are required to provide assistance for the enforcement of criminal law and laws imposing pecuniary penalties (and other purposes), but does not generally extend to the enforcement of civil law.

Importantly, Sections 313(5) and (6) of the Act include provisions to ensure that C/CSPs and their officers, employees or agents are "not liable to an action or other proceedings for damages for or in relation to an act done or omitted in good faith" in relation to providing this assistance to law enforcement agencies.

Equally, Section 314 allows C/CSPs to recover the costs that they have incurred in providing the required assistance.

In addition to the website blocking that C/CSPs provide under Section 313 of the Act, Internet Services Providers (ISPs, note that CSPs include ISPs) are required to block access to overseas websites that infringe copyrighted content where copyright owners have been granted an injunction by the Federal Court under the *Copyright Amendment (Online Infringement) Act 2015*.

**Technical issues**

It should be noted that, independent of any underlying regulation or legislation, website blocking is a relatively blunt tool and has the potential for comparatively easy evasion by offending website operators as well as internet users. It also has the potential to result in inadvertent 'over-blocking', thereby impacting the websites and content of many other legitimate entities, including schools, universities, libraries and cloud-based services, in ways that may hamper their legitimate activities and disadvantage consumers.

This was the case in the so-called ASIC-incident in 2013, where the use of Section 313 of the Act to request blocking of a single website also resulted in the unintended blocking of 250,000 additional websites (refer to Sections 2.20 to 2.25 of the report *Balancing Freedom and Protection*[5] prepared by the House of Representatives Standing Committee on Infrastructure and Communications).

As a result of this Inquiry and report, in April 2016, Government published the *Australian Government draft guidelines for the use of section 313(3) of the Telecommunications Act 1997 by government agencies for the lawful disruption of access to online services*[6] (Guidelines).[7] The Guidelines seek to establish good practice measures for Government agencies. Those measures include a minimum level of authority when using the powers under Section 313, appropriate internal policies and procedures including a complaints and review process, the provision of information on each blocking (including 'stop pages') to the

[5] 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

[6] See https://www.communications.gov.au/have-your-say/guidelines-lawful-disruption-access-online-services

[7] We note that it appears that no final Guidelines have been issued since the release of the draft Guidelines in April 2016.

general public, consultation with ISPs prior to making blocking requests and, importantly, the required technical expertise to ensure no 'over-blocking' nor other unwanted side-effects of blocking occur.

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

Moreover, it should be noted that site blocking is relatively easily circumvented by internet users who 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 or purpose-built programs. Please refer to *Annex A: Means to circumvent website blocking* for further details.

Note also that the Australian two-year mandatory data retention regime, which has been in full effect since April 2017, has made consumers more aware of the fact that their communications history is now captured and stored. Consequently, more tools that allow the use of the internet 'without surveillance' are coming into the market and are becoming popular in the mainstream community as everyday tools. Many of those tools are equally useful where users wish to circumvent website blocking. Some VPN service providers report an increase of usage of their services by over 100%. Privacy advocates also promote the use of VPNs, as recently done by Digital Rights Watch, which declared 13 April the 'National Get A VPN Day'.[8]

[8] http://digitalrightswatch.org.au/2017/04/12/get-a-vpn/

# 3. Proposed Civil Penalties Regime

As highlighted above, Communications Alliance seeks to confine its comments on Recommendation 14:

> Should the Commissioner be able to seek a court order to require Internet Service Providers (ISPs) to block individual website(s) in extreme cases where all other avenues have been exhausted?

Against the background of the current legal framework for website blocking, the technical issues associated with it and the limited effectiveness of website blocking highlighted above, we note the following:

1. "This discussion paper suggests the establishment of a prohibition against the sharing of intimate images without consent and the introduction of a civil penalty regime targeted at those involved in the sharing of these images, as well as the content hosts. The prohibition would be included in legislation, such as within the *Enhancing Online Safety for Children Act 2015* (Cth) (EOSC Act)."

   It is not clear to us what is being envisaged with regards to the legislation that, under a civil penalties regime, would enable the Commissioner to seek a court order to require ISPs to block websites: Is it being envisaged that the civil penalties regime itself includes such powers, or would the required powers be included in the EOAS Act, or is the thinking to increase the scope of Section 313 of the Act to include civil matters, or something else?

2. In considering the need to apply website blocking, it should be noted that it may not be possible to block all websites containing the images under consideration due to the nature of the internet and the ability of the community to further share images across a vast range of websites. Many business models of pornography related websites rely on the linking of images and videos to other content, thereby spreading any material further than might have been originally intended by the poster. Equally, other websites might actively troll the internet for newly uploaded intimate images and link to any new content that has been found. Consequently, the party that originally posted the intimate images may have no knowledge, let alone control, over the dissemination of the images over the internet. In this context, it is important to understand that C/CSPs are unable block access to individual parts of popular websites, e.g. C/CSPs cannot block access to a specific Facebook user while allowing access to all other Facebook users.

3. Irrespective of the underlying legislation, Industry points out that the principles of indemnity and cost recovery as currently included in Section 313 of the Act must be mirrored in the enabling legislation. This is especially important as image sharing might involve some extremely popular websites which, if blocked, are likely to cause great user and content host dissatisfaction. It appears also likely that the number of cases where such blocking could be requested is not insignificant, therefore making the recovery of costs (or rather, as previously suggested, the payment of a fee upfront) an important consideration for Industry.

4. It is equally important to ensure that the mistakes made in the ASIC incident and other incidents are not repeated on what might be a much larger scale, given the proliferation of image sharing and social media. The measures outlined in the draft Guidelines regarding the use of Section 313 of the Act would need to apply to the Commissioner's Office irrespective of the underlying legislation. We reiterate that the measures currently contained in the Guideline, which leaves sufficient room for evasion by Government agencies, rather ought to be contained in the respective legislation itself.

5. Importantly, the Commissioner's Office should be required to acquire the necessary technical expertise to ensure no 'over-blocking' occurs and website blocking is as accurately targeted as technically possible (but note the concerns around the effectiveness of blocking raised in the previous section and Annex A). In this scenario, the Commissioner's Office should also be required to provide adequate resources to facilitate consultation with ISPs, education of the general public and a complaints/review process. Under no circumstances must ISPs be placed in a situation that requires judgement on their part of whether or not a breach of the sharing prohibition has occurred, i.e. ISPs must merely be the executors of a technically clearly defined order and bear no liability for any resulting claims for damages.
6. Given the inherent technical issues and limited effectiveness of website blocking, the enabling legislation ought to expressly limit its use to a measure of last resort as set out in Recommendation 14. The legislation ought to include a clear 'escalation' and approvals process that must be followed prior to seeking a court order for website blocking.

**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 online safety and cyber security debate.

Industry recognises the creation of the Office of the eSafety Commissioner as an important measure to a coordinated national approach. However, an overarching framework combining cyber security and online safety ought to consider how the use of the illegal or socially undesirable use of the internet and the sharing and exposure to potentially harmful content – beyond non-consensual sharing of intimate images – can be minimised without undue limitation of citizens' rights and freedoms.

It should be noted that no amount of content control is likely to completely eliminate potential harm to citizens from occurring as a result of the use of the internet and other forms of digital communications. Therefore, it is much more important to teach the public in general, and children in particular, appropriate online behaviour. This ranges from issues such as the disclosure of personal information, non-consensual (or even consensual) sharing of explicit photos, cyber-bullying etc. to the consumption of content which may have detrimental effects on a person's physical, social and emotional wellbeing.

It appears that there is already a vast amount of useful information available to the public. Notably, with the establishment of the Office of the eSafety Commissioner, a national Government agency has 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.

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 may 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 would welcome continued engagement with the Department of Communications and the Arts and other stakeholders on the proposed creation of a civil penalties regime for non-consensual sharing of intimate images and online safety and cyber security in general.

Given some of the issues surrounding the blocking of websites, Industry would welcome timely consultation on any draft legislation should the proposal of a civil penalties regime be further pursued.

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

# ANNEX A: 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.

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.

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