COMMUNICATIONS
ALLIANCE LTD

Communications Alliance Submission

to the Attorney-General's Department
in response to the

Copyright Enhancement Review

7 March 2023

INTRODUCTION

This submission represents the views of Carrier/Carriage Service Provider (CSP) and Digital Platform members of Communications Alliance Ltd.

Communications Alliance welcomes the opportunity to provide a submission to the Department of the Attorney-General's Copyright Enforcement Review Issues Paper.

In the submission we respond directly to a selected number of the questions posed in the Issues Paper.

Members of Communications Alliance may also make individual submissions in response to the review.

About Communications Alliance

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

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

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

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

.

QUESTIONS IN DISCUSSION PAPER

Question 1: *What challenges have you been facing in relation to copyright infringement in recent years? Are you seeing any changes or trends (including any forms or methods of infringement that are emerging or particularly concerning, or conversely, are becoming less prevalent or concerning)?*

Looking beyond copyright infringement, we submit that copyright law needs to be updated to enable innovative technological uses that are beneficial for society and the economy. In particular, Australia's copyright law does not include fair dealing exceptions for:

- Artificial Intelligence (AI) / Text and Data Mining (TDM);
- Incidental and Technical Use;
- Archival, Caching and Display; and
- Cloud Computing and Personal Use Copying.

Another option that could be considered is a move to a broader principles-based exception, along the lines of the US "fair use" framework.

Question 4: *Are the currently available industry-led mechanisms appropriate, and/or being appropriately used, to address or prevent actual or potential copyright infringement? Which mechanism(s) are most frequently and/or effectively used, and why?*

Section 115A website blocking scheme

Eradication of copyright infringement altogether will likely remain unachievable.

Nonetheless, the current mechanisms and industry tools for addressing copyright infringement are working well.

For example, the Copyright Act's website blocking scheme (Section 115A), has been the subject of multiple Federal Court decisions, including decisions to extend existing orders. This mechanism generally operates effectively and offers a relatively straightforward means for rights holders to request CSPs to block access to sites that infringe or facilitate the infringement of copyright. CSPs worked in good faith with rights holders to agree a standard set of orders in the first two applications, to ensure a consistent approach, and to obviate the need for CSPs to appear in subsequent proceedings, thereby reducing the costs for all parties.

The streamlined process for applications that are extensions or variations of already existing injunctions, for example to extend an injunction to additional top-level domains, is also proving efficient.

At present the blocking that occurs pursuant to court orders is at the DNS level and it is important that this is maintained and that any proposed technical solutions or requirements are feasible and scalable for CSPs.

Industry-led approaches

Digital platforms have also been proactive ins seeking to protect copyright.

For example, Google proactively removes pirate websites from its search results as well as blocking proxy or mirror sites. This has been reported in the press, including:

- Content Cafe, 15 December 2020, *The fight against piracy continues during a tumultuous year*
    - *"Google ramps up efforts in fight against piracy - In a significant move for the tech company, Google Australia agreed to voluntarily remove more than 800 pirate websites and block any proxy sites that reappear. The support of tech companies like Google is essential in the fight against piracy and this local achievement is being closely watched internationally."*

- Sydney Morning Herald, 27 August 2020, *Google moves to block movie piracy loophole*
    - *"Google Australia has agreed to banish hundreds more websites involved in the illegal downloading of movies and programs after pirates were able to bypass its initial attempts to remove them from search results. The tech giant agreed to voluntarily pull down websites engaging in piracy last year to help stop the spread of illegally downloaded material, a move which allowed copyright holders to avoid fighting the tech giant for an injunction in court. However, content pirates were able to reappear on Google by slightly tweaking the domain address and creating "proxy" or "mirror" sites - variations of the previously blocked addresses."*

Meta also takes a proactive approach to detecting and removing infringing material on its services. According to its latest Transparency Report, more than 87 per cent of copyright infringing material was removed proactively by Meta, without requiring a report from a rightsholder. It also works with industry stakeholders across the world to identify and disable websites that may be dedicated to piracy or to facilitating copyright infringement and prevents ads from appearing on apps and websites associated with piracy.

Meta also provides innovative tools to help creators and advertisers identify and report infringing material, including Rights Manager - a tool specifically designed to help content owners protect their rights and manage their content at scale.

Question 6: *Are the costs (including financial and time costs), benefits and risks of industry-driven mechanisms appropriately shared between different parties?*

See answer to Q.8

Question 8: *How effective and efficient is the current website blocking scheme as a way of combating copyright infringement and steering online consumers towards legitimate sources of content? For example, is the application process working well for parties, and are injunctions operating well, once granted?*

Website blocking should not be seen as a "silver bullet" to combat online copyright infringement. It will only ever be one mechanism as part of a multi-faceted approach to reducing copyright infringement. These approaches also need to include education about copyright and availability of content, at attractive prices and in a convenient and timely manner. The Productivity Commission in its Final Report on Intellectual Property Arrangements highlighted that "what has

appeared to limit infringement is timely and competitively-priced access to content." [1] Rights holders, their publishers and other content providers are best placed to bring content to Australian consumers in a timely and competitively priced way. This approach is the most efficient and effective way to reduce online copyright infringement.

We are not aware of any s115A application or extended blocking order that has been refused by the Federal Court. These applications are also being dealt with relatively swiftly by the Courts.

The blocking process itself is not necessarily simple for all CSPs to implement. For this reason, CSPs' costs, which include administrative costs of legal oversight and technical implementation, are not always fully met by the current provision for costs set out in the Court orders. CSPs should not be responsible for the costs associated with enforcement. Rights holders must bear the cost of enforcing their own property rights. It is not appropriate for there to be any changes reducing the amount rights holders may be ordered to pay CSPs for implementing blocks.

In fact, the legislation should be amended to expressly provide that the CSPs' costs of complying with an injunction should be borne by the copyright owner. (Similarly, section 314 of the *Telecommunications Act 1979* provides that CSPs should not bear the costs of complying with requests for assistance from enforcement agencies.)

For the website blocking scheme to operate efficiently, it should continue to minimise the need for CSPs to contest the application, including through ensuring that a CSP is not liable for any costs unless it enters an appearance and takes part in the proceeding.

There should not be any proposal to reduce the compensation element of the scheme.

In relation to digital platforms, there has been significant investment in order to make reporting as simple and seamless as possible for rightsholders. Digital platforms also work to be as proactive as possible, including by investing in detection technology and building partnerships with rightsholders.

Question 9: *Could the way the website blocking scheme operates be improved in any way (for example to address the use of new and emerging technologies to navigate around or through website blocks), including through changes to how the current scheme is practically implemented, or potential amendments to legislation?*

From the CSPs perspective, the legislation should ensure that orders made by the Court are clear, so they can be efficiently implemented. It is in no one's interest that there be uncertainty about what amounts to taking reasonable steps. Some CSPs report that, at times, a lack of clarity in the orders requires the CSP to interpret those orders. Courts presently also make orders in multiple formats, which is not ideal for the recipients and should be corrected.

CSPs are not aware of any practical or reasonable changes to section 115A that would prevent users "navigating around" website blocks. A website block will deter some people from visiting those sites to access infringing content and educate as to why a site has been blocked. The Department's latest report on its consumer survey on online copyright infringement notes that 60% of respondents simply gave up when they encountered a blocked website. Those who had not encountered a blocked website in the past 3 months (67%) were also asked what they would do if they were to be faced with such a scenario. As was the case for those who had experienced this, most claimed they would just give up (72%)[2]

[1] pp. 568/569, Productivity Commission, *Intellectual Property Arrangement, Productivity Commission Inquiry Report*, as accessed at:https://www.pc.gov.au/inquiries/completed/intellectual-property/report/intellectual-property.pdf on 7 March 2023

[2] pp 105/106 Orima (commissioned by the Attorney-General's Department) *Consumer Survey on Online Copyright Infringement 2022, Survey Findings Report*, as accessed at: https://www.ag.gov.au/system/files/2023-02/consumer-survey-on-online-copyright-infringement-2022_report.pdf on 7 March 2023

We acknowledge that sophisticated or determined users may be circumventing the blocks, via relatively simple means such as not using their ISPs' default DNS settings or using VPNs. These are not new or emerging technologies, but long-understood limitations to website blocking as a method for reducing infringement. In 2014, Justice Arnold in the UK commented:

> *"blocking of targeted websites has proved reasonably effective in reducing use of those websites in the UK. No doubt it is the casual, inexperienced or lazy users who stop visiting those websites, whereas the experienced and determined users circumvent the blocking measures."*[3]

The review correctly notes, though, that the likely primary use of these tools is not to circumvent content blocks, but "to increase the speed, reliability, security, and customisablity of the user's internet experience". In Question 9, the review asks if the website blocking scheme could be improved, e.g., via addressing these technologies, and if so, what are the broader or unintended consequences that should be considered.

From our perspective, a significant and grave unintended consequence of regulating VPNs and DNS is the negative impact to a secure, private, and open Internet. The Internet was not built with security or privacy in mind, and daily we see examples of just how critical Internet security and privacy are for Australians. Many of these types of tools were developed by global technology providers and disseminated widely for the express purpose of enhancing an individual's online privacy and security – these tools are able to do so by significantly minimising the exposure of sensitive data and protecting user privacy and personal information. Many VPNs and DNS tools are essential for helping to achieve the critical objective of increasing Internet privacy and security for Australians and global citizens.

Additionally, VPN and DNS are widely used across the world in locations where Internet freedoms are curtailed. Australia's regulation of these technologies, even under the premise of protecting copyright, would be a strong signal to other governments that it is permissible, even acceptable, for them to also do so for goals unrelated to copyright – there is a worrying trend of authoritarian jurisdictions regulating VPNs and DNS with the intent of curtailing rights and freedoms. Australia taking any actions to regulate VPN and DNS technologies would essentially justify these repressive actions and potentially set off a cascade of copycat rules around the globe. Question 9 creates another concern that the Australian government could potentially require technology companies to build new and "improved" blocking technologies, which would only further bolster the total blocking abilities of regimes that actively seek to curtail Internet rights and freedoms.

We strongly urge the Attorney-General to consider these broader impacts to both Australia and global online rights and freedoms when evaluating the appropriateness and proportionality of regulating VPNs and DNS, which are essential in ensuring a private, secure and open Internet.

Question 10: *How effectively and efficiently are the authorisation liability provisions and/or safe harbour scheme (and associated notice and take-down process) currently operating as mechanisms for addressing copyright infringement? For example:*

Authorisation liability provisions

Authorisation liability laws are robust and no change is needed. We do not support any change to section 101 that would reverse the High Court's decision in the iiNet case.

Following the Redbubble Australia decision, Australia has one of the strictest authorisation laws in the common law world.

[3] Ref: Cartier International AG & Ors v British Sky Broadcasting Limited & Ors [2014] EWHC 3534 (Ch) at [236]

There have been numerous claims made by rights holders in the past that authorisation law is "broken" and not capable of addressing online piracy or capable of applying to digital platforms. We do not agree with these assertions.

Three of the most recent cases on authorisation law in Australia involved digital platforms, and the platform or online service provider was found to have authorised copyright infringement in these cases:

- *Cooper v Universal Music* -where a website operator was found to have authorised the infringements of users of the site.
- *Universal Music v Sharman* - where Kazaa, the peer-to-peer music sharing software was found to have authorised the copyright infringements of Kazaa users.
- *Pokémon Company v Redbubble* - where Redbubble was found to have technically authorised infringements uploaded by users of the marketplace, despite the Judge explicitly stating that Redbubble had done all that it could to address infringing third party content. Redbubble was found liable, but nominal damages of $1 were ordered due to Redbubble being a 'good actor' re its take down processes and systems design. Redbubble was ordered to pay Pokemon's costs.

Safe harbour scheme

Copyright safe harbours are critical – they incentivise service providers to work with rights owners to remove infringing content, whilst providing safeguards for users. Currently, the safe harbour system is available to internet access providers and certain other institutions, including education collecting institutions. The protections offered by the safe harbour scheme should be extended to include all online service providers. As noted by the Productivity Commission in its Final Report on Intellectual Property Arrangements:

> *"In the Commission's view, extending the coverage of Australia's safe harbour regime, along the lines proposed in the Australian Government's exposure draft amendments, will improve the system's adaptability as new services are developed. Such an expansion is consistent with Australia's international obligations and is an important balance to the expanded protections for rights holders Australia has accepted as part of its international agreements. As such this is a legislative amendment that should be made without delay.*
>
> *RECOMMENDATION 19.1 The Australian Government should expand the safe harbour scheme to cover not just carriage service providers, but all providers of online services. and amend the definition of a service provider under s116ABA of the Copyright Act"*[4]

This expansion is the appropriate mechanism for addressing any shortcomings in digital platforms' notice-and-takedown regimes. These platforms are already heavily incentivised to combat infringement and develop close partnerships with rights holders, and there is no proven need to put in place any separate, mandatory, enforcement regime.

Copyright law in Australia should be updated and brought in line with more expansive safe harbour schemes in jurisdictions such as the United States which has the *Digital Millennium Copyright Act* (DMCA). The DMCA is a useful precedent for Australia, as it establishes parameters for online services which balances the interests of rights holders and their ability to take steps against content that infringes their copyright, with certainty and processes allowing online services to methodically respond to claims of infringing content on their services. This could easily occur by Australia building on the existing safe harbour scheme and expanding it to all providers of online services. Without adequate safe harbour frameworks, Australia remains a jurisdiction with risks for online services hosting content.

[4] p. 567, Productivity Commission, *Intellectual Property Arrangement, Productivity Commission Inquiry Report*, as accessed at:https://www.pc.gov.au/inquiries/completed/intellectual-property/report/intellectual-property.pdf on 7 March 2023

There is a range of views among CA members as to the utility of the tiered arrangements for authorisation liability under section 116 of the Act.

Some members believe that the arrangements should be updated to ensure that the safe harbours are fit for the purpose of digital innovation and service provision. They believe that reliance on specific categories of activity and the need to satisfy specific conditions for each category in order to qualify for safe harbour is overly complex and rigid and creates uncertainty about "gap cases" that may not clearly fall within these categories.

It is understood that these arrangements implement Australia's trade related commitments under the Australia-US FTA. However, one CSP submits that the objective of the scheme could still be achieved by revising Division 2AA to provide a general safe harbour to a "service provider" that is not aware of copyright infringement on networks within their control. The availability of the safe harbour would not depend on what type of activity the service provider was in engaged in as currently required but rather the response of the service provider once they are notified of infringement on networks/services over which they have the ability (and right?) to control.

Some CA members recommend, however, that the distinctions between activities – e.g. hosting, cache and conduit – be maintained, because they align with global copyright regimes and are a recognition of the actual capabilities of these types of providers to remove online infringing material, depending on their role in internet infrastructure. A caching provider, for instance, cannot remove infringing material that it does not host and caching services are not necessary for the content's availability online. Should these critical distinctions be erased, global service delivery and processes for managing copyright infringement claims would need to be completely overhauled, at considerable cost, due to the significantly heightened exposure to copyright infringement claims.

Published by:
COMMUNICATIONS
ALLIANCE LTD

Level 12
75 Miller Street
North Sydney
NSW 2060 Australia

Correspondence
PO Box 444
Milsons Point
NSW 1565

T 61 2 9959 9111
F 61 2 9954 6136
E info@commsalliance.com.au
www.commsalliance.com.au
ABN 56 078 026 507