Response to the Australian Government Discussion Paper: Online Copyright Infringement

Joint Submission
1 September 2014
## Contents

1. Introduction 3
2. A legislative response is required 5
3. Extended authorisation liability 8
   - The current scheme 8
   - Deficiencies in the current authorisation scheme 11
   - International comparisons 13
   - Deficiencies in Proposal 1 – Extended authorisation liability 14
   - Response to Questions 1-5 15
4. Extended injunctive relief to block infringing overseas sites 22
   - The current scheme 23
   - International experience 24
   - Effectiveness and proportionality 26
   - Costs and other considerations 28
   - Compliance with Australia’s international obligations 30
5. Extended safe harbour scheme 32
   - The current scheme 33
   - Deficiencies in the current safe harbour scheme 34
   - Deficiencies in Proposal 3 – Extended safe harbour scheme 36
   - Response to Questions 7-11 38
   - Building the evidence base 40
1 Introduction

1 The Australian Screen Association (ASA), the Australian Home Entertainment Distributors Association (AHEDA), the Motion Picture Distributors Association of Australia (MPDAA), the National Association of Cinema Operators (NACO) and the Australian Independent Distributors Association (AIDA) (collectively, the Australian Film/TV Bodies), are pleased to make this submission in response to the Australian Government’s discussion paper Online Copyright Infringement (the Discussion Paper).

2 These associations represent a large cross-section of the film and television industry that contributed $6.1 billion to the Australian economy and supported an estimated 49,000 FTE workers in 2009-10:1

(a) The ASA represents the film and television content and distribution industry in Australia. Its core mission is to advance the business and art of film making, increasing its enjoyment around the world and to support, protect and promote the safe and legal consumption of movie and TV content across all platforms. This is achieved through education, public awareness and research programs, to highlight to movie fans the importance and benefits of content protection. The ASA has operated in Australia since 2004 (and was previously known as the Australian Federation Against Copyright Theft). The ASA works on protecting and promoting the creative works of its members. Members include: Village Roadshow Limited; Motion Picture Association; Walt Disney Studios Motion Pictures Australia; Paramount Pictures Australia; Sony Pictures Releasing International Corporation; Twentieth Century Fox International; Universal International Films, Inc.; and Warner Bros. Pictures International, a division of Warner Bros. Pictures Inc.

(b) AHEDA represents the $1.3 billion Australian film and TV home entertainment industry covering both packaged goods (DVD and Blu-ray Discs) and digital content. AHEDA speaks and acts on behalf of its members on issues that affect the industry as a whole such as: intellectual property theft and enforcement; classification; media access; technology challenges; copyright; and media convergence. AHEDA currently has 12 members including all the major Hollywood film distribution companies through to wholly-owned Australian companies such as Roadshow Entertainment, Madman Entertainment, Hopscotch Entertainment and Anchor Bay Home Entertainment.

(c) The MPDAA is a non-profit organisation formed in 1926 by a number of film distribution companies in order to promote the motion picture industry in Australia. It represents the interests of motion picture distributors before government, media and relevant organisations, providing policy and strategy guidance on issues such as classification, accessible cinema, copyright piracy education and enforcement and industry code of conduct. The MPDAA also acts as a central medium of screen-related information for members and affiliates, collecting

---

and distributing film exhibition information relating to box office, admissions and admission
dresses, theatres, release details and censorship classifications. The MPDAA represents Fox
Film Distributors, Paramount Pictures Australia, Sony Pictures Releasing, Universal Pictures
International, Walt Disney Studios Motion Pictures Australia and Warner Bros.

(d) NACO is a national organisation established to act in the interests of all cinema exhibitors. It
hosts the Australian International Movie Convention on the Gold Coast, this year in its 69th
year. NACO members include the major cinema exhibitors Amalgamated Holdings Ltd, Hoyts
Cinemas Pty Ltd, Village Roadshow Ltd, as well as prominent independent exhibitors Pacific
Cinemas, Dendy Cinemas, Grand Cinemas, Nova Cinemas, Cineplex, Wallis Cinemas, Ace
Cinemas and many other independent cinema owners. NACO represents over 1,600 cinema
screens throughout Australia, New Zealand and the Pacific regions.

(e) AIDA is a not-for-profit association representing independent film distributors in Australia, being
film distributors who are not owned or controlled by a major Australian film exhibitor or a major
U.S. film studio or a non-Australian person. Collectively, AIDA’s members are responsible for
releasing to the Australian public approximately 75% of Australian feature films which are
produced with direct and/or indirect assistance from the Australian Government (excluding
those films that receive the Refundable Film Tax Offset).

3 All of the Australian Film/TV Bodies and their members have a vital interest in a strong and effective
protection of their copyright assets in Australia and the ability to enforce their copyright against threats
of online infringement. Indeed, companies represented also invest heavily in major Australian
productions that generate millions of dollars in revenue and many thousands in employment. Online
copyright infringement presents one of the biggest challenges to the film and television industry’s
participation in the Australian digital economy, and its contribution to the broader Australian economy.
Whilst collectively we embrace digital distribution models and the concept of making content available
sooner and on multiple platforms (and for feature films often first available in Australia before the rest
of the world), online copyright infringement is also preventing legitimate online business models for the
distribution of films and television programs from reaching their full potential.

4 This is a critical opportunity for Australian laws and practice around online copyright protection to be
brought into line with best practice around the world, after past missed opportunities, and to remedy
unanticipated problems with Australian copyright laws that have impeded the development and
implementation of an effective scheme to prevent infringement.

5 The creative industry sector is committed to working with the Government and other stakeholders to
develop a legal framework which ensures that there are effective and flexible processes in place to
protect copyright online. There are a number of proposals being put forward in this consultation
process from differing representatives from the creative industries. Whilst these proposals may take
differing approaches, they are put forward to achieve the same outcome – to ensure there is an
effective legal framework and the necessary legal incentives for service providers and rights holders to
work together to ensure the Copyright Act will continue to support creative content owners and those
who invest in them to continue to invest in and produce creative content to meet legitimate consumer expectations.

2 A legislative response is required

6 Australians have become internationally infamous as being among the most active internet pirates of television and movie content, according to one source having the highest rates per capita of unauthorised downloads of a recent Game of Thrones season finale, and the highest percentage of overall downloads of the Breaking Bad finale, despite each episode being available in Australia on the same day as the US and priced at only a few dollars. The Attorney General has publically recognised that Australia is the "worst offender of any country in the world" when it comes to internet piracy.  

7 This is despite the fact that the content industries have ensured the ready availability of online digital platforms and education of consumers on where they can acquire legitimate digital content. Recent Australian research has found that consumers recognise that there is a wide array of online legal services available with 74% of persistent illegal downloaders agreeing that there are an increasing number of options for people to legally obtain and watch movie and TV content online. 72% of Australian adults that engage in piracy say that, in the absence of piracy, they would access content legally by going to the cinema (23%) or waiting for it to be legally available on TV, online or on DVD (50%).

8 There is strong evidence to suggest that users know full well that distributing files over the internet is illegal: for example, a 2013 quantitative study carried out by Sycamore Research for the Intellectual Property Awareness Foundation (Sycamore Study) found that 67% of Australian adults expressly agreed that downloading or streaming pirated content is stealing or theft. The Sycamore Study also provides evidence of consumer support for injunctive relief legislation, with the majority of adults agreeing that Australian courts should be allowed to decide to block overseas websites that solely profit from copyrighted content (with 44% of persistent illegal downloaders agreeing with this preventative solution).

9 The problem of online copyright infringement cannot be tackled by rightsholders on their own. Litigation against individual infringers, or even against individual websites (which, as the Discussion Paper acknowledges, are “predominantly based overseas”) is not a practical or effective solution.

---

5 Intellectual Property Awareness Foundation and Sycamore Research, Research into the online behaviour and attitudes of Australians in relation to movie and TV piracy, Research Summary, 2013 (print publication).
6 2014 Sycamore research, to be released in Q3 2014.
7 Intellectual Property Awareness Foundation and Sycamore Research, Research into the online behaviour and attitudes of Australians in relation to movie and TV piracy, Research Summary, 2013 (print publication).
8 Intellectual Property Awareness Foundation and Sycamore Research, Research into the online behaviour and attitudes of Australians in relation to movie and TV piracy, Research Summary, 2013 (print publication).
Any practical solution to online copyright infringement needs to target the elements over which we, as Australians, have control: namely, the internet connection via which unauthorised copies of works are being made available to and are being accessed by local consumers en masse. This is a principle which the Australian Government has already accepted: as acknowledged in the Discussion Paper, the legislative scheme introduced by the Digital Agenda Act (DAA) in 2000 is "intended to create a legal incentive for service providers such as ISPs to take reasonable steps to prevent or avoid an infringement where they are in a position to do so".

It is also a principle that is reflected in Australia’s international obligations regarding the proper scope for ISP liability for copyright infringement. As described in paragraphs 20 to 21 below, the basic scheme of Australian law in this area (as introduced by the DAA) is based on Australia’s obligation under Art. 8 of the WIPO Copyright Treaty (WCT) to provide rightsholders with a technologically neutral right of communication to the public, on the condition that “the mere provision of physical facilities for enabling or making a communication does not in itself amount to communication”. In this way, Art. 8 of the WCT – which was enacted in order to deal with the challenges of a digitised world – sets up the basic balance between the rights of copyright owners and the proper limits on liability of communications service providers such as ISPs when it comes to dealing with online infringements. As a contracting party to the WCT, Australia is required to respect this balance in its domestic copyright law (and has historically done so, being one of the first countries to implement Art. 8).  

These obligations under the WCT have since been substantially reinforced by Australia’s entry into binding treaty commitments under its free trade agreements with the US, Singapore and Korea. As the Discussion Paper correctly recognises, these treaties require Australia to “provide a legal incentive to ISPs to cooperate with rights holders to prevent infringements on their systems and networks” (p 3). Specifically, all three treaties require Australia to provide “legal incentives for service providers to cooperate with copyright owners in deterring the unauthorised storage and transmission of copyrighted materials”.  

The free trade agreements with the US and Korea note that this is “for the purposes of providing enforcement procedures that permit effective action against any act of copyright infringement” (emphasis added). The US-Australia agreement goes so far as to include specific side letters on the topic of ISP liability, which demonstrates the importance of this topic to, and the seriousness with which it is regarded by, the Australian government. These binding international obligations are relevant to evaluating potential areas for reform of existing Australian copyright laws.

During the decade following the introduction of the DAA reforms, copyright owners have fully tested the effect of current Australian laws to deal with systemic online copyright infringement. This included civil and criminal investigations of those responsible for operating pirate websites from Australian

---

9 See paragraph 20 below.
10 Australia-US Free Trade Agreement, Art 27.11(29); Australia-Singapore Free Trade Agreement, Art. 12(1); Australia-Korea Free Trade Agreement (not yet in force), Art. 13.9 (29).
computer systems, civil cases against the operators of P2P systems\(^\text{12}\) and claims successfully brought where there were attempts to monetise infringing traffic, including by an Australian ISP.\(^\text{13}\)

\labeledref{14} However, the High Court’s decision in *Roadshow Films Pty Ltd & ors v iiNet Ltd*,\(^\text{14}\) (the *iiNet decision*) has seriously curtailed attempts to prevent and minimise online copyright infringement by finding that the current copyright framework does not require an ISP, in the position of iiNet in that case, to take steps to prevent known infringements occurring on its network (as long as it is not itself directly involved in the infringing activity). This has greatly undermined the legislative purpose of the existing scheme, and has removed incentives for ISPs to cooperate with rights holders to address online copyright infringement, contrary to Australia’s international obligations. As all members of the High Court in the *iiNet decision* recognised in their conclusions, there is a clear need for a legislative response to online copyright infringement.

\labeledref{15} The majority of the High Court stated that:\(^\text{15}\)

> “This final conclusion shows that the concept and the principles of the statutory tort of authorisation of copyright infringement are not readily suited to enforcing the rights of copyright owners in respect of widespread infringements occasioned by peer-to-peer file sharing, as occurs with the BitTorrent system. The difficulties of enforcement which such infringements pose for copyright owners have been addressed elsewhere, in constitutional settings different from our own, by specially targeted legislative schemes, some of which incorporate co-operative industry protocols, some of which require judicial involvement in the termination of internet accounts, and some of which provide for the sharing of enforcement costs between ISPs and copyright owners.”

\labeledref{16} The minority judges also saw the need for a legislative solution to deal with new circumstances:\(^\text{16}\)

> “The history of the Act since 1968 shows that the Parliament is more responsive to pressures for change to accommodate new circumstances than in the past. Those pressures are best resolved by legislative processes rather than by any extreme exercise in statutory interpretation by judicial decisions.”

\labeledref{17} The Australian Film/TV Bodies and other rights holders have also undertaken extensive negotiations with ISPs (some with input from government), in an attempt to negotiate an industry based cooperative solution to address online infringement. Those negotiations began well before *Roadshow v iiNet* and details of the attempts to negotiate emerged in the evidence in that case and were acknowledged by the Full Federal Court.\(^\text{17}\) This included development of draft industry codes and meetings between representative bodies until it was clear that the position of the ISPs was that no member “should be required to take any action against their customers who are engaging in copyright infringement over their networks” and there was no utility in further negotiations in view of that stance.\(^\text{18}\)

\labeledref{12} *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* [2005] FCA 1242 (5 September 2005) (*Kazaa*).

\labeledref{13} *Cooper v Universal Music Australia Pty Ltd* [2006] FCAFC 187 (18 December 2006) (*Cooper*).

\labeledref{14} [2012] HCA 16 (20 April 2012) (*Roadshow v iiNet*).

\labeledref{15} *Roadshow v iiNet* at [79].

\labeledref{16} *Roadshow v iiNet* at [120].

\labeledref{17} *Roadshow v iiNet* [2011] FCAFC 23 (24 February 2011) at [281]-[283].

\labeledref{18} *Roadshow v iiNet* at [283].
More recent negotiations since the iiNet decision – brokered by the government - have been well and truly exhausted (with one key ISP walking away entirely). It is now time for a legislative solution, preferably one that allows the possibility of further negotiations over more detailed and effective cooperative processes. Given the extensive economic impact of internet piracy on the Australian film and television industry (and the consequent impact on the broader Australian economy), there is an urgent need for the Government to legislate.

3 Extended authorisation liability

Proposal 1—Extended authorisation liability

The Copyright Act would be amended to clarify the application of authorisation liability under sections 36 and 101 to ISPs.

In determining whether a person has authorised an infringing act, a court would still be required to consider the nature of the relationship between the person authorising the infringement and the person who did the infringing act, and whether the person took any reasonable steps to prevent or avoid the infringing act (as currently required).

In making an assessment of the ‘reasonable steps’ element, a court must have regard to:

(a) the extent (if any) of the person’s power to prevent the doing of the act concerned;
(b) whether the person or entity was complying with any relevant industry schemes or commercial arrangements entered into by relevant parties;
(c) whether the person or entity complied with any prescribed measures in the Copyright Regulations 1969; and
(d) any other relevant factors.

The ‘power to prevent’ the infringing act would no longer be a separate element, but would be only one of a number of relevant factors in determining whether ‘reasonable steps’ were taken to prevent or avoid the infringement. The amendments would clarify that the absence of a direct power to prevent a particular infringement would not, of itself, preclude a person from taking reasonable steps to prevent or avoid an infringing act.

The Australian Film/TV Bodies endorse the policy objective expressed in the Discussion Paper that “Extending authorisation liability is essential to ensuring the existence of an effective legal framework that encourages industry cooperation and functions originally intended, and is consistent with Australia’s international obligations.” (DP, p3). The current scheme has failed to meet its stated objectives and amendments to the Act are required to put it on the correct path.

The current scheme

When enacted in 2000, the legislative scheme under the DAA – which included amendments to authorisation liability – was one of the most advanced legislative schemes for protecting copyright online anywhere in the world.¹⁹ During the Second Reading Speech, the Attorney General described

¹⁹ Neither the US nor Canada had implemented a right of communication to the public at this time. The WCT, Art 8 of which provides for a right of communication to the public, did not come into force anywhere in the world until 6 March 2002.
the DAA amendments as intended to “update Australia’s copyright standards to meet the challenges posed by rapid developments in communications technology, in particular the huge expansion of the Internet” and being “at the cutting edge of online copyright reform and clearly [placing] Australia among the leaders in international developments in this area”. The Parliamentary Secretary for the Minister for Communications, Information Technology and the Arts echoed these comments in relation to the revised Bill.

The key components of the scheme were the introduction of a new technologically neutral right of communication to the public (as mandated by Art. 8 of the WCT), the amendment to the authorisation provisions to introduce a new mandatory three factor test (e.g. s101(1A)) and the introduction of a limited defence for the operators of facilities (e.g. s112E) in line with the agreed statement relating to Article 8 of the WCT. The scheme was clearly intended to apply to ISPs, as the Explanatory Memorandum (EM) explained:

(a) The “outline” referred to the role of telecommunications carriers and ISPs in “the delivery of content and the operation of the information economy”, and said that the Bill “provides greater certainty about the responsibilities of carriers and ISPs to copyright owners and the steps they need to take to avoid infringing copyright” (emphasis added).

(b) The “regulation impact statement” contained some key passages indicated that “given the important role that ISPs in particular play in facilitating access by Australians to online services and electronic commerce, legislation providing for liability for copyright infringements in the online environment ought to be clearly defined and fairly applied.

(c) One of the objectives of the amendments contained in the Bill was to ensure that the law “provides carriers and carriage service providers (including ISPs) with reasonable certainty about liability for infringements that occur on their facilities or infrastructure”. Within the framework of the proposed amendments, the first issue was “the liability of carriers and carriage service providers (including ISPs) for infringements on their facilities” and a distinction was drawn between direct infringement and infringement by authorisation.

20 Second Reading Speech for Copyright Amendment (Digital Agenda) Bill 1999, 2 September 1999, Senate pp 9748-9750.
21 Second Reading Speech for Copyright Amendment (Digital Agenda) Bill 2000, 14 August 2000, Senate pp 16245-16247.
22 To replace the technology-specific broadcasting right and the limited diffusion right, which would encompass the “making available of copyright material online.” Explanatory Memorandum to Copyright Amendment (Digital Agenda) Bill 1999, p 3.
23 And the corresponding provisions under s36(1A) and s 39B).
24 Explanatory Memorandum to Copyright Amendment (Digital Agenda) Bill 1999, p 4.
25 Explanatory Memorandum to Copyright Amendment (Digital Agenda) Bill 1999, p 6 (Part 1.1).
26 Explanatory Memorandum to Copyright Amendment (Digital Agenda) Bill 1999, p 7 (Part 2.1).
27 Explanatory Memorandum to Copyright Amendment (Digital Agenda) Bill 1999, p 9 (Part 3.1).
28 Explanatory Memorandum to Copyright Amendment (Digital Agenda) Bill 1999, p 9 (Part 3.1).
Three options were considered in relation to liability for authorising copyright infringement, ranging from leaving the Act unchanged to codification of “the principles set out in the authorisation case law”, together with “a limitation on liability for authorisation for carriers and carriage service providers (including ISPs)”. The EM expressed the view that, if no amendments were made, “ISPs might find themselves liable for authorising copyright infringements by doing no more than providing facilities for persons transmitting copyright material without permission of the copyright owners”. The latter option was chosen and was reflected in s101(1A) and s112E (and the corresponding provisions for works). The policy objective was “so that carriers and carriage service providers (including ISPs) would not be liable for authorising infringements that occur on their networks, including on web sites hosted on their servers but operated independently of the ISP, by reason only of the fact that the infringements occurred on the facilities provided by the carrier or carriage service provider (including ISPs)”.

This is in line with the Agreed Statement in relation to Art. 8 of the WCT, which relevantly acknowledges “that the mere provision of physical facilities for enabling or making a communication does not in itself amount to communication within the meaning of this Treaty or the Berne Convention”.

The EM also described the effect of the s101(1A) in the draft Bill: “The inclusion of these factors in the Act essentially codifies the principles in relation to authorisation that currently exist at common law (see in particular University of New South Wales v Moorhouse (1975) 133 CLR 1). It is intended to provide a degree of legislative certainty about the steps that should be taken in order to avoid liability for authorising infringements. Additional certainty in relation to third party liability is provided by new s.101(1A)(c). This section specifies that compliance with relevant industry codes of practice is a factor in determining whether the person took reasonable steps to prevent or avoid the doing of the act”.

The scheme was supplemented by the introduction of the safe harbours for ISPs in 2005, to implement Australia’s obligations under the Australia-United States Free Trade Agreement (AUSFTA). Article 17.11 of the AUSFTA provided that “for the purposes of providing enforcement procedures that permit effective action against any act of copyright infringement” the parties would provide:

(a) “legal incentives for service providers to cooperate with copyright owners in deterring the unauthorised storage and transmission of copyrighted materials”; and
(b) limitations “regarding the scope of remedies available against service providers for copyright infringements that they do not control, initiate, or direct, and that take place through systems or networks controlled or operated by them”.\textsuperscript{34}

23 The requirements of Article 17.11 recognised the role of ISPs in preventing infringements of copyright online and the proposed limitations to remedies where the ISP did not control, initiate or direct the infringements of copyright – they did not provide ISPs with a general immunity from remedies and did nothing to limit the liability of ISPs for acts of infringement they did not control. Article 17.11.29(b) also made detailed provision for the categories of internet activity to be covered, the nature of the limitations on remedies, and the conditions to be met by a service provider to qualify for the protection of the provisions. These are reflected in the current Div 2AA of Part V of the Act.

Deficiencies in the current authorisation scheme

24 Although the existing scheme has been applied in a number of cases – primarily where the parties accused of authorising infringements were very closely involved in the infringing acts\textsuperscript{35} – the true test of whether it had achieved its purpose was the iiNet decision in 2012. In that case, the ISP was found not to be liable for authorising infringements by users of its network when it refused to take any action to stop account holders from infringing copyright.

25 Although the High Court recognised the important change to authorisation introduced in s101(1A), which was an “express requirement” (at [68]), it interpreted the scheme (including the existence of s112E and the safe harbours) as imposing no liability for inactivity in the face of infringements taking place on its network. The Court decided that:

(a) there was no “statutory warrant” to impose a positive obligation on the ISP to act (at [59]) and that the rights holders’ case assumed “obligations on the part of an ISP which the Copyright Act does not impose” (at [77]). As long as an ISP had no direct power to prevent the infringements, even if it “supported” or “encouraged” its customers to continue to infringe and refused to exercise its contractual rights against the subscribers, it would not authorise.\textsuperscript{36} It did not matter that there was evidence of widespread infringement occurring on the ISP’s network;\textsuperscript{37}

(b) the “nature of the internet”, the way in which the subscribers infringed copyright (using the BitTorrent system which post-dated the DAA) and the “absence of any industry code” applying to all ISPs, made it reasonable for the ISP to do nothing in the face of infringements;\textsuperscript{38}

\textsuperscript{34} Australia-United States Free Trade Agreement, Article 17.11, para 29.
\textsuperscript{35} E.g. Cooper and Kazaa.
\textsuperscript{36} Majority at [69] and [70].
\textsuperscript{37} 50\% of iiNet’s traffic was BitTorrent (at [38] and [92]).
\textsuperscript{38} Majority at [71] and [76].
(c) s112E – the provision enacted to give effect to Australia’s obligations under the agreed statement in relation to Art 8 of the WCT – is redundant because under Australian law it “appears to provide protection where none is required”.

(d) the fact that the ISP had been found not to qualify for the safe harbours – because it had not implemented any policy in relation to repeat infringers, by taking steps to prevent infringement – was irrelevant because the ISP was not liable in the first place by taking such steps.

26 The Discussion Paper describes the effect of the decision as to “severely limit the circumstances in which an ISP can be found liable for authorising an act by a subscriber that infringes copyright.” The Australian Film/TV Bodies agree with that conclusion. The fact that there is no evidence of any systemic action being taken against online infringements by ISPs since the iiNet decision, and that ISPs have been unwilling to negotiate any industry code, suggests that the ISPs have reached the same conclusion.

27 The result of the iiNet decision is contrary to the legislative intent of the DAA, which was to provide certainty as to the steps that were required by an ISP to prevent online infringement of copyright, or face the prospect of liability for authorisation, in line with Australia’s international obligations. It also renders the three most important components of the scheme – the factors in s101(1A), the defence under s112E and the safe harbours – irrelevant and unnecessary. Liability under the scheme was never specified to be dependent on whether an ISP had “direct power” over infringers – s101(1A) contemplated reasonable steps that could include an industry code amongst ISPs, s112E contemplates that the provider may only provide a facility and the safe harbours assume that the ISP does not have direct control over the infringing acts.

28 It is artificial – and unconvincing – to suggest that an ISP cannot take any action to prevent infringement by users of its services. ISPs have the contractual right to stop a subscriber from misusing their services and could clearly discourage infringing use of the services if they decided to do so. As the Discussion Paper recognises, even without direct power to prevent infringement, there still may be reasonable steps that an ISP can take “to discourage or reduce online copyright infringement.” The schemes that are in operation in other countries (outlined below in paragraphs 30 and 32) are confirmation of this conclusion. The High Court clearly recognised that there were steps available to an ISP to prevent infringement.

29 Australia should act to correct the problem with the existing authorisation framework in order to fulfil the legislative intent of the DAA and also because it is the right thing to do in the face of rampant piracy in Australia. This will also ensure that Australia is compliant with its international treaty

39 Majority at [26].

40 Explanatory Memorandum to the Copyright Amendment (Digital Agenda) Bill 1999 (Cth), pp 4, 8, 14-15.
obligations (which, as discussed at paragraphs 12 and 14 above, is no longer the case following the iiNet decision).

**International comparisons**

30 As well as ensuring that Australia is compliant with its binding international obligations, revising and updating the current authorisation scheme would also put Australia (once a leader in international copyright developments) back into line with international practice in this area. The clearest example of this is the proliferation in other jurisdictions of legislative or voluntary schemes that allocate responsibility for dealing with online infringements of copyright between rightsholders and ISPs. These schemes, known as ‘graduated response schemes’, are based on a clear allocation of responsibility to ISPs that do not (by complying with the scheme) take steps to address copyright infringement by their users. While this allocation of responsibility does not receive significant attention in most discussions of graduated response schemes, common sense dictates that the schemes would be unlikely to exist (much less be complied with by ISPs) in the absence of this basic incentive structure.

31 Korea was an early adopter of such an incentive structure. In 2008, the Korean content industry faced massive online piracy and the home entertainment sector had shut, with the loss of 7,200 jobs. Cinema and film production were facing a bleak future. The problem became so serious that it caused competitors in private enterprise that normally “sparred” with one another to coalesce with government support and as a matter of urgency bring about a solution that worked. Today Korea has one of the healthiest film and TV industries in the world. The combined initiative of the Korean Government and private enterprise was a combination of three powerful initiatives: a) an inspired education campaign, b) legal content made available online in a timely manner and at attractive prices, and c) effective government legislation. While the Korean legislation is not a template for Australia, given that the two countries have very different legal and social structures, the Korean economic example shows what can be achieved if legislation is effective in ensuring that ISPs and rights holders both address the issues.

32 The Discussion Paper refers to the voluntary schemes in place in the US and the UK, and the statutory graduated response scheme in NZ, as examples of such “specially targeted legislative schemes”. While the Australian Film/TV Bodies agree that these are comparators, the Government should also be aware that graduated response schemes are currently in place in a total of eight countries. There are flaws in a number of these models, predominantly around the allocation of costs and lack of effective mitigation measures which, if mirrored in Australia, would make such a scheme ineffective and unlikely to be used. A scheme that was discussed at length during the rightsholder/ISP discussions was the US voluntary notice scheme – one in which each side bears its own costs and has effective mitigation measures. The US scheme began operating 18 months ago, in February

---

41 US, UK, NZ, France, Taiwan, South Korea, Canada and Ireland. The Irish scheme involves only the largest Irish ISP, Eircom, and is the result of a confidential settlement of litigation between Eircom and rightsholders.
It is time for Australia to clarify the application of authorisation liability to ISPs to provide a basis for a similar graduated response scheme here.

**Deficiencies in Proposal 1 – Extended authorisation liability**

33 The Australian Film/TV Bodies support the intention of Proposal 1 to clarify the application of authorisation liability under the Copyright Act to ISPs, but do not support the form of Proposal 1.

34 There are a number of problems with Proposal 1, including:

(a) The increased importance attached to the relationship between the alleged authoriser and the primary infringer (because of the reduction in importance of power to prevent) would do little to assist interpretation unless there is some form of definition to guide the Court in the meaning to attach to different relationships.

(b) The relocation of the first factor under s101(1A) – “power to prevent” – to being a factor under reasonable steps is very unlikely to change the interpretation placed on that concept by the High Court in the iiNet decision. It was the content of the power to prevent that limited the steps that were reasonable, not its location or ordering within the set of three factors.

(c) The inclusion of a new open-ended phrase “any other relevant factors” has the potential to create far greater uncertainty than the existing provisions, by bringing in any other factors that the Court considers on the day would be relevant, and these need not be limited to factors within copyright law or otherwise related to the statutory scheme.

(d) The proposal to clarify that absence of direct power to prevent would not preclude a finding of authorisation falls short of what is required after iiNet – a provision confirming that the power to prevent can include both a direct and indirect power would be far more useful.

(e) The inclusion of two potential measures of compliance – the Code and the Regulations – could be problematic, as they may be given equal and conflicting weight by a Court, particularly if they are in different terms (as would be expected given their different origins).

35 Because it involves a substantial change to the statutory language, the Proposal also has the potential to reopen previous decided interpretations. There is an existing important body of law that has developed around the application of the existing 3 factors under s101(1A). The High Court recognised in iiNet that the provisions had been applied in a number of cases – Kazaa, Cooper - which recognised the rights of copyright owners against certain types of authorisers of online infringers. Any change to the 3 factor test would run the risk that these authorities could be re-litigated in future cases. This is an undesirable outcome not only for the parties involved, but also in terms of judicial economy and legal certainty.

---

42 *The Copyright Alert System, Phase One and Beyond*, CCI, 28 May 2014.
A better solution – which ensures that the amendments are targeted at overcoming the problems with the *iiNet* decision which involves ISPs – would involve less radical changes to the existing language of the section and the inclusion of several other provisions and definitions which would operate as deeming provisions. These would include a definition clarifying that power to prevent would include both direct and indirect power and definitions around the nature of the relationship which would recognise the significance of contractual relationships and the power that they provide to prevent or avoid online piracy.

A new provision would deem authorisation to occur where an ISP fails to take reasonable steps – which are also defined inclusively to include compliance with a Code or Regulations – in response to infringements of copyright it knows or reasonably suspects are taking place on its network. Deeming provisions are well known in the Copyright Act, as is the concept of reasonable suspicion (which has been the subject of a number of decisions). A provision in this form would provide great clarity, for ISPs and copyright owners alike, around the steps that an ISP would be required to take to avoid a finding of authorisation and provide the very kind of incentive that is required for the ISP to cooperate in the development of a Code.

There is another important omission from Proposal 1: it does not address the need for amendment to s112E, the facilities provider defence. The High Court made clear in the *iiNet* decision that the Court’s ultimate conclusion was based on the interpretation of the existing authorisation liability scheme under s101(1A) construed with s112E. Section 112E has been a problematic provision, in part because of the use of the words “merely because” – words which have been given different interpretations. s112E has been considered by a number of judges – some treating it as changing a result that otherwise would follow under authorisation principles and others as being unnecessary because it relates to a position that would fall short of authorisation. In the *iiNet* decision, the High Court reached the latter view: the judges observed that it “appears to provide protection where none is needed” and that it “seems to have been enacted from an abundance of caution.”

Any extension of the authorisation liability scheme will need to also amend s112E to prevent a situation where the benefits of extending authorisation under s101(1A) are undermined by the current interpretation of s112E – that inaction by an ISP in the face of infringement using its services is not (without more) authorisation.

**Response to Questions 1-5**

**QUESTION 1:** What could constitute ‘reasonable steps’ for ISPs to prevent or avoid copyright infringement?

It will be important for any set of ‘reasonable steps’ to be flexible and adaptable to changes in technology. One solution in the short to medium term is to oblige the ISP under the code to consider

---

*Roadshow v *iiNet* at [69]*

*Roadshow v *iiNet* at [26] and [113].
other technical options that may become available to it in future, especially in relation to mitigation 
measures. There will also need to be a more general understanding that the code or regulations 
setting out the reasonable steps may need to be substantially revised in light of the technological 
changes that are likely to occur in the medium and long term.

41 It would be open to the Government to prescribe a similar set of ‘reasonable steps’ in the relevant 
regulations, or indeed in legislation, if an industry code is not agreed. The Australian Film/TV Bodies 
have no objection to this course of action if it becomes necessary. This could be achieved indirectly, 
for example by providing that, despite the rest of s 101(1A), ISPs will be liable for authorising 
infringements of copyright on their networks of which they had actual knowledge if there is no industry 
code in force after a prescribed date. Alternatively, the Government could fix a date on which it will 
prescribe a statutory code if an industry code has not been agreed by then.

42 Once the authorisation liability scheme is amended to make clear that ISPs will be liable for 
infringements of copyright by their subscribers which they know about but do not take reasonable 
steps to prevent or avoid, an industry code prescribing the content of those ‘reasonable steps’ is likely 
to be agreed between rightsholders and ISPs without excessively protracted negotiations. This is 
because, once the incentive for ISPs to cooperate is in place, there is increasing international 
precedent for, and consensus about, the type of steps that can be cooperatively taken by ISPs and 
copyright owners to address online copyright infringements and which effectively balance the interests 
of all stakeholders, including consumers.

43 A good example of contemporary practice and one that is supported by the Australian Film/TV Bodies 
is the US Copyright Alert System, in which ISPs and rights holders bear their own costs. This system 
provides for a range of “reasonable steps” – ranging from educational notices sent to account holders 
through to technical measures (known as mitigation measures) that can be taken by ISPs to address 
repeat infringers who have reached the stage of more severe notices.45

> Depending on the service provider, the ISP’s range of actions may include:
> • A temporary reduction in Internet speed;
> • A temporary downgrade in Internet service tier; or
> • Redirection to a landing page for a set period of time, until a subscriber contacts the ISP 
or until the subscriber completes an online copyright education program.

44 Under the US scheme there are an escalating series of notices that reflect these different types of 
steps that can be taken by ISPs. The notices escalate if infringement continues up to six notices; the 
first and second notices alert the subscriber that infringement is happening, being primarily educative; 
the third and fourth notices require active acknowledgement by the subscriber; while the fifth and sixth 
notices come with “mitigation measures,” such as temporarily reduced Internet speeds. The 
combination of initial educative notices and some technical responses are key to having an effective 
set of measures.

45 http://www.copyrightinformation.org/the-copyright-alert-system/what-is-a-copyright-alert/
Though still relatively nascent the US Copyright Alert Scheme has been working. The effectiveness of these measures has been confirmed in the recent report issued by the CCI to coincide with the first anniversary of the scheme: The Copyright Alert Scheme: Phase One and Beyond. The report found that there was a substantial reduction in the need for further notices being sent to account holders after the initial educative notices had been sent, which is consistent with the fact that the scheme is:

“...based on the premise that most consumers will take corrective action if alleged copyright infringement involving their Internet account is brought to their attention. This theory is supported by research regarding consumer attitudes that was conducted on CCI’s behalf both prior to the program’s launch and also more recently. In our recent survey, we found that 79% of respondents believe that the receipt of an Alert would be “somewhat” or “very influential” in getting them to stop engaging in infringing behavior. Our focus group research completed in the summer of 2012, found similar attitudes.”

Nevertheless, the effectiveness of the scheme depends on the potential for there to be escalated responses if the infringing activity continues on an account – the presence of notices alone without more would not be as effective. The US Copyright Alert System leaves a significant level of discretion to the individual ISP to determine of the range of mitigation measures – shaping, throttling or redirection – which it will impose. This flexibility in approach is appropriate to enable a scheme to have the widest possible adoption throughout the industry through its ability to be adapted to the different practices of different ISPs.

In the event that it becomes necessary to legislate an industry code for ISPs, the Australian Film/TV Bodies recommend that such a code be included in the Telecommunications Act 1997 (Cth). A code given force under this Act would have mandatory effect and create a level playing field for all ISPs. This may be necessary if ISPs contest the application of extended authorisation liability, as in light of the iiNet case, a code that forms part of the Copyright Act may not be sufficient. However, if the safe harbour scheme was extended beyond ISPs, this could create a two tier regulatory scheme, which applies only to ISPs rather than other non ISP service providers that are not subject to the Telecommunications Act.

Whatever the legal mechanism adopted, the above principles provide solid guidance as to the content of a scheme that will be workable and acceptable to all stakeholders regarding the necessary ‘reasonable steps’. Both a voluntary code and a regulatory scheme would be equally capable of being revised as necessary to address technological changes, provided that the required flexibility is built in from the beginning.

---

47 The Copyright Alert System, Phase One and Beyond, CCI, 28 May 2014.
48 CCI Report, p 2.
QUESTION 2: How should the costs of any ‘reasonable steps’ be shared between industry participants?

49 The original legislative scheme under the DAA dealt with the costs of taking action to prevent infringements of copyright and how they would be shared, as the EM recorded:49

“Owners of copyright would bear the costs of monitoring compliance with their new rights and taking civil actions to enforce those rights. Owners would also bear the costs of the proposed exceptions to the proposed new right of communication to the public. …

Under Options A, B and C, carriers and carriage service providers (including ISPs) would bear the cost of becoming aware of any new laws relating to liability for authorisation of breaches of copyright. They would also bear the cost of taking any relevant measures to avoid liability. However, the costs and uncertainty to carriers and carriage service providers (including ISPs) under Options A and B would probably be higher than under Option C.”

50 The Australian Film/TV Bodies support the extension of these principles of cost sharing into any new industry code or regulatory scheme regarding ‘reasonable steps’. It reflects the reality of such a scheme in a way that reaches an appropriate compromise between all stakeholders, i.e. that each group bears the costs that are an incident of their own operations in relation to the ‘reasonable steps’ scheme. Copyright owners would pay their own costs of identifying the infringements and notifying these to the ISP, while ISPs would bear the costs of matching the IP addresses in the infringement notices to subscribers, issuing the notices and taking any necessary technical mitigation measures.

51 This is a rational approach to meeting the costs of a scheme. It means that the parties with the control over steps in the process – rightsholders have control over the investigative steps, which ISPs have control over the account matching, notice-issuance and technical mitigation steps – have the incentive to control and can control the costs of those steps. Seeking to change that balance would involve obvious problems, with the potential that one of the parties would have no incentive to keep costs down because it knew the other party was liable, or worse still could seek to profit from their steps in the process if they knew they could try to charge for it. This would give rise to a need for a range of complex problems including determination of the real costs (as opposed to the claimed costs), obligations of transparency and a need to audit the process to verify the costs actually incurred – conditions that have never been agreed. The problems would result even if legislation sought to impose other than a costs-sharing approach, as occurred with the UK statutory graduated response scheme which was never acted upon due to its associated high costs.

52 A cost-sharing approach is consistent with the US Copyright Alert System, in which the costs of implementation are “divided equally between rights holders and ISPs”. The rightsholders pay for the costs of investigation of infringing conduct of which there are considerable costs including the investigative steps, including managing and updating a set of keywords and titles for the use in the investigation, verification of the infringing file using file hash techniques or other processes (manual, watermarks or fingerprints) and delivery of case information for each investigation to the relevant ISP

49 Explanatory Memorandum to Copyright Amendment (Digital Agenda) Bill 1999, pp 13-14 (Part 4.2.1).
in a form capable of being processed by the ISP with the minimum effort. The ISP then electronically matches the information with the relevant account and this leads to generation of the notices to the account holders and any mitigation measures if there is repeat conduct.

53 This type of costs sharing arrangement also reflects the fact that the costs of reasonable steps should be assessed in relative terms and balanced with the benefits from improved copyright protection. As the EM to the DAA recognised in 2000: the “benefits of the proposed amendments to owners of copyright and the community generally outweigh the disadvantage of possibly increasing the costs of using copyright material in the communications networks and the Internet”.

54 The NZ Infringing File Sharing Act (IFSA) graduated response law is an example of a poorly designed and poorly implemented copyright alert scheme. The scheme imposed a very high set price per notice issued by an ISP - $25 - to be paid by rightholders. Rightholders did not support such a payment scheme and informed the NZ government that this was the wrong approach and the cost imposed by the scheme was uneconomic and would result in few notices being issued. The flaws in the scheme were apparent from the total lack of any transparent process used to determine the real cost to the ISPs, the lack of transparency in its implementation and the absence of any auditing of the amounts charged by ISPs. Anecdotal evidence indicates that the cost charged by some ISPs generates a profit for them.

55 These flaws meant that very little use has been made of the NZ scheme. The NZ music industry, who describe the notice scheme as “complicated and costly” has sent a total of 12,345 detection notices between August 2012 and August 2014 – equating to a mere 128 notices per week. Eighteen (18) cases have ended up in the Copyright Tribunal with an average deterrent penalty being handed down of NZ$523 - equating to 3.58% of the maximum penalty (NZ$15,000) that the Copyright Tribunal could award. Research has found that the impact of the NZ scheme was very short-lived following the media coverage of the legislation and saw a gradual rise to levels of BitTorrent infringement which surpassed the pre-legislation levels.

**QUESTION 3:** Should the legislation provide further guidance on what would constitute "reasonable steps"?

56 Given the interpretation given to the concept of reasonable steps under s101(1A) by the High Court in the iiNet case, there should be a legislative recognition of the reasonable steps that are referred to in the response to Question 1 above to avoid a repetition of the result in that case that removed any incentive for ISPs to take action of any kind in the face of infringements known to be occurring on their networks.

57 The High Court failed to acknowledge what both common sense and research indicate – such as the research in the US Copyright Alert scheme that found that – that many internet users would stop

---

50 Explanatory Memorandum to Copyright Amendment (Digital Agenda) Bill 1999, p 16 (Part 4.4).
52 http://www.nbr.co.nz/stayconnected?return=158477
engaging in infringing activity if they were sent a notice indicating that they had been identified and that the notice scheme included effective mitigation measures for those internet users who continued to infringe. Clearly, issuing educational notices (such as the notices in stages 1 and 2 of the US Copyright Alert Scheme) should have legislative recognition as reasonable steps. So too would notices that require active acknowledgment from the account holder before they are able to continue to use the internet service.

58 Statutory recognition of reasonable steps would importantly also include the types of mitigation measures that have already been implemented in the US Copyright Alert Scheme, such as temporary reduction in internet speed, temporary downgrade of internet package or redirection to a landing page until the account holder contacts the ISP. These measures are already being successfully used by ISPs when they seek a change in behaviour by an account holder – evidence of their effectiveness in deterring or reducing the undesirable behaviour which would support their use in a legislated graduated response scheme introduced in Australia.

59 Given that the US Copyright Alert Scheme is example of a scheme developed cooperatively by rightsholders and ISPs which has a design and implementation that both groups support (structure, graduated levels of response with effective mitigation measures, consumer group involvement, a review mechanism and cost-sharing etc), an equivalent scheme ought to be capable of being introduced into Australia. However, in the absence of any current intention of and incentive for ISPs in Australia to support such a scheme (and the strong opposition from some ISPs), legislative recognition of the reasonable steps involved in such a scheme is necessary.

60 On the other hand, the Australian Film/TV Bodies would support a form of legislation that leaves open the opportunity within a clearly defined and limited timeframe for rightsholders and ISPs to design and implement a scheme in Australia that would not only be recognised under the Copyright Act (as an industry code is currently capable of being recognised under s101(1A)) but would take precedence over the bare legislated steps – allowing a degree of flexibility in its implementation and an ability to respond to changes in technology more quickly than a purely statutory scheme. Such an approach would be consistent with the policy intention of the government stated in the Discussion Paper of seeking to encourage the development of an industry code in response to online infringement.

QUESTION 4: Should different ISPs be able to adopt different ‘reasonable steps’ and, if so, what would be required within a legislative framework to accommodate this?

61 As indicated in the response to Question 1 above, the Australian Film/TV Bodies believe that any industry or regulatory code regarding reasonable steps should give ISPs flexibility to select from a list of effective mitigation measures, along the lines of the US Copyright Alert Scheme. There could also be flexibility in how different ISPs implement the codified graduated response scheme, provided that they follow the basic principles.

62 ISPs could have a discretion regarding the number of early-stage notices that they issue and the language of these notices – as occurs in the case of the US Copyright Alert scheme. Allowing ISPs
flexibility in how they implement a graduated response scheme and manage their own customers, provided that they follow its key principles, is a proportionate and balanced solution that is most likely to be acceptable to all stakeholders.

63 This issue is closely related to Question 3, because a legislative scheme that is flexible enough to allow ISPs to choose between various reasonable steps measures would depend on there being a defined set of measures that would constitute reasonable steps in the first place. Assuming such a set of measures is described in the Copyright Act, the same amending legislation could also provide that these would amount to reasonable steps.

**QUESTION 5:** What rights should consumers have in response to any scheme or ‘reasonable steps’ taken by ISPs or rights holders? Does the legislative framework need to provide for these rights?

64 The Australian Film/TV Bodies recognise the need for consumers to have confidence in any graduated response scheme implemented in Australia. This includes confidence in the technical processes that are used to identify infringing activity and match the activity to account holders, the confidence that their personal information is not disclosed in the process and the confidence that there is an opportunity for consumers to challenge circumstances where they believe that they have been wrongly identified. Effective graduated response schemes, such as the US model, address each of these concerns.

65 Best practice online investigations utilise mature technologies and investigation techniques that are highly reliable in detecting infringing activity and capturing sufficient information about it (including IP addresses, dates and times, evidence of file transfer etc) to support an account matching exercise. These technologies and techniques have been proven repeatedly in both civil and criminal cases coming before the Courts in recent years. They were employed in a number of the cases referred to below in relation to Proposal 2.

66 In the case of the US Copyright Alert Scheme, there is a single designated form of investigation that meets high standards of accuracy and probity and has been accepted by consumer groups and ISPs as sufficient evidence in order for an account matching process to be undertaken. Independent expert assessment was carried out in relation to the efficacy of the processes to “monitor, identify, collect evidence and generate notices to P2P infringers” and it found that the methodologies effectively identified online infringers, were well-developed, involved evidence collection that was “robust, defensible and will withstand adverse party scrutiny or evidentiary challenges and includes appropriate checks and balances”.53

67 The data matching process only involves the use of information gathered from the public domain about the infringing activity – details of the IP address of the user identified as engaging in infringing activity – which is then provided to the relevant ISP controlling the range of IP addresses within which this IP

address falls. The ISP then carries out an exercise to match the IP address details to the relevant account based on the IP address allocated at the time of the alleged infringing activity. In this way none of the personal details (name, address etc) of the account holder are disclosed to rightsholders.

68 Once the account matching has taken place and a notice is issued to an account holder, there is a formal process providing consumers with the opportunity to query the allegations in the notice and request an independent review of the information. A recently published empirical analysis of the review process for the first year of operation of the US Copyright Alert Scheme found that there was an extremely small number of consumer challenges to notices.54

Over the first nine months of the program, 0.27% of the Alerts eligible for review by AAA were actually challenged – and we believe this fact reinforces the reliability of the notice and Alert generation process. Of those requests for review that were filed, the AAA was able to confirm that in no cases did any Alerts mistakenly identify the details associated with an infringement or mis-identify the account being associated with an Alert. In fact, the Alert/s and applicable Mitigation Measures were upheld in 77% of the cases. In the remaining cases, 18% were settled in favor of the subscriber based primarily on the demonstration that his or her account had been used without authorization.

69 The central concept of effective mitigation measures, cost allocation and review mechanisms behind the US Copyright Alert Scheme would be appropriately included in any legislative or industry code implemented in Australia. Rightsholders in Australia already have access to the type of investigative techniques used under the US Copyright Alert Scheme.55 Rightholders have never sought access to the private account information of the accounts affected under a graduated response scheme and would not need access to such information to make the scheme effective. The scheme would also be transparent and, where appropriate, offer an independent review process to allow users to challenge notifications they believe were sent in error.

4 Extended injunctive relief to block infringing overseas sites

Proposal 2—Extended injunctive relief

The Copyright Act would be amended to enable rights holders to apply to a court for an order against ISPs to block access to an internet site operated outside Australia, the dominant purpose of which is to infringe copyright.

Rights holders would be required to meet any reasonable costs associated with an ISP giving effect to an order and to indemnify the ISP against any damages claimed by a third party.

70 The Australian Film/TV Bodies support the proposed extension of injunctive relief to block infringing overseas websites in the Discussion Paper. This is a vital development, overdue under Australian

54 The Copyright Alert System, Phase One and Beyond, CCI, 28 May 2014, p 10.
55 The company carrying out the evidence gathering process in iiNet later became the unit within MarkMonitor that carries out the investigations on behalf of the rightsholders under the US Copyright Alert Scheme.
copyright law, for tackling the predominantly criminal supply of infringing content that Australian infringers do access.

The current scheme

71 Notorious websites, such as Pirate Bay, represent the first destination for Australian internet users to obtain torrent files for unlicensed content to enable them to download that content from other P2P users. Despite enforcement action being taken against the founders of the site in their countries of origin, the nature of these websites is that the physical infrastructure of the site can be moved between countries and the operators may be on the run even after they are prosecuted. These websites are invariably located outside Australia – as Australian sites have shut down as a result of earlier enforcement activity by rightsholders.

72 The current scheme under the Copyright Act leaves copyright owners without an effective remedy against large and often profitable criminal websites operating outside Australia. Remedies for copyright infringement – including injunctions – follow from findings of liability against the organisation to be enjoined. As the iiNet decision confirmed, unless they can first establish liability against an ISP for authorising infringing activities by account holders using its services, Australian Courts will not grant an injunction to require an Australian ISP to block access to an overseas pirate website regardless of the impact that that website is having as an illegal supply channel for unlicensed content in Australia.

73 This is in spite of the fact that the safe harbour provisions introduced into the Copyright Act in 2005 specifically provide for the Court to order an ISP found liable for authorising to block an overseas website (see s 116AG (3A). No application for an injunction under that provision has ever succeeded. For the reasons explained above in relation to Proposal 1 (i.e. the limited scope for authorisation liability for ISPs under Australian law post the iiNet case), there is currently little prospect that an Australian ISP will be found liable for authorising infringing online activity of its account holders and that the trigger required for a site blocking order under the safe harbours would arise.

74 The problem facing rightsholders is that there is no so-called no-fault based injunction available to them under Australian copyright law to require an ISP to block even the most notorious overseas criminal website. The benefits of such a no-fault injunction are clear – it would be independent of a finding of fault by an ISP. Not being the target of a finding against it, an ISP is unlikely to oppose the injunction – as long as the procedural requirements for the injunction are met. Once made, a blocking injunction would immediately prevent Australian internet users from being tempted to or accessing the

56 Despite having been sentenced to eight months’ imprisonment for copyright infringement by Swedish Courts in 2009, Pirate Bay co-founder, Peter Sunde, was only recently arrested after having been on the run for more than 2 years.
58 It was uncovered during the 2009 criminal trial of The Pirate Bay that its expenses were an estimated USD$110,000, yet the site’s advertising revenues were USD$1.4 million - equating to gross illegal profit margins of 1,272%.
blocked sites. The simplicity, directness and effectiveness of this approach would have the capacity to significantly reduce online infringement in Australia. The absence of a no-fault procedure may explain the very high rates of film and TV piracy in Australia when compared with European countries that have such a procedure.

International experience

A large number of European countries have implemented and applied legislation that enables site blocking, including Ireland (referred to in the Discussion Paper and considered further below), Belgium (VZW BAF v NV Telene), Italy (Bergamo Public Prosecutor’s Officer v Kolmisappi), Sweden (Columbia Pictures Industries Inc v Portlane AB), Denmark (Telenor v IFPI) and IFPI Danmark v Tele 2 A/Ø, and Austria (Constantin Film v UPC).

In the United Kingdom, a site blocking provision has been used to currently block 40 separate foreign websites on the basis of copyright infringement. Section 97A of the Copyright, Designs and Patents Act 1988 empowers the English High Court “to grant an injunction against a service provider, where that service provider has actual knowledge of another person using their service to infringe copyright”. The jurisdiction to grant a site blocking injunction depends on the existence of s97A, as explained by Henderson J when applying the provision to block access to four infringing websites earlier this year:

“… under English law an injunction cannot normally be granted against a person against whom no substantive cause of action exists. Authority to do so, therefore, was specifically provided in section 97A.”


The Information Directive contains a number of important recognitions of the importance of a framework for protecting copyright online: the need for increased certainty, “providing for a high level of protection of intellectual property” that is crucial to intellectual creation, providing an appropriate level of reward and the opportunity for satisfactory returns on investments and the need for member states to provide for effective sanctions and remedies for infringements of rights.

The Information Directive also recognised the reality of the online environment that.

---

59 United Kingdom, Germany, Spain, Finland, France, Iceland, Italy, Norway, Portugal, Ireland, Netherlands, Sweden, Belgium, Denmark, Austria and Russia
60 http://help.sky.com/articles/our-approach-to-protecting-copyright
61 Paramount Home Entertainment v British Sky Broadcasting [2014] EWHC (Ch) 18 February 2014 (Paramount v BskyB) at [8].
62 Information Directive recitals (2)-(4), (7)-(16).
63 Information Directive recitals (58)-(60).
“In the digital environment, in particular, the services of intermediaries may increasingly be used by third parties for infringing activities. In many cases such intermediaries are best placed to bring such infringing activities to an end. Therefore, without prejudice to any other sanctions and remedies available, rightsholders should have the possibility of applying for an injunction against an intermediary who carries a third party’s infringement of a protected work or other subject matter in a network … even if the acts carried out by the intermediary are exempted [from liability].”

80 Art 8(3) of the Information Directive provides that:

“Member States shall ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right.”

81 The Enforcement Directive is also an important instrument recognising the need for effective enforcement measures to enable rightsholders to protect their copyright in the online environment. Art 8(3) of the Enforcement Directive provides that:

“1. Member States shall provide for the measures, procedures and remedies necessary to ensure the enforcement of the intellectual property rights covered by this Directive. Those measures, procedures and remedies shall be fair and equitable and shall not be unnecessarily complicated or costly, or entail unreasonable time-limits or unwarranted delays.

2. Those measures, procedures and remedies shall also be effective, proportionate and dissuasive and shall be applied in such a manner as to avoid the creation of barriers to legitimate trade and to provide for safeguards against their abuse.”

82 Since the first order under s 97A was made on 28 July 2011 (requiring British Telecom to block access to the “Newzbin 2” website (Twentieth Century Fox Film Corp & Ors v British Telecommunications Plc [2011] EWHC 1981 (Ch) (BT case))), a well settled body of jurisprudence has developed governing s 97A applications. This has now evolved to the point where Henderson J in the 2014 case referred to at paragraph 76 above only required 44 paragraphs to grant the requested order which (as is now usual practice) was not opposed by the ISP defendants (see judgment at [4]). The reality in the UK today is that all applications for site blocking injunctions brought by the content industries are the “obvious cases” referred to by the Discussion Paper as occasions for industry cooperation (p 6).

83 The UK cases granting injunctions under s 97A have unanimously found that the type of site blocking requested by the rightsholders was technically feasible (and in many cases already in use) and not excessively costly to the ISPs (see e.g. BT case at [177]). The usual method of internet blocking ordered by the English High Court is known as “IP address blocking”. This is a way of blocking access whereby internet traffic destined for a given IP address (for example The Pirate Bay or Newzbin2) is sent down a non-existent or NULL route.64 The user receives a message that the webpage is unavailable, effectively rendering access to that site blocked. IP address blocking is a common method of preventing access to banned websites and can be particularly effective where there is an easily identifiable target with an IP address that is known and not shared with other non-infringing

64 For example, to block www.example.com.au, the DNS for “.example.com.au” would be modified, but any address with “.com” and/or “.au” would be unaffected. This can be an effective method to target a site such as The Pirate Bay as the DNS “thepiratebay.se” is easily identifiable and is not shared.
The largely consensual nature of s 97A cases in practice is unsurprising, given that their focus is not on the conduct of ISPs (other than to ascertain that they are service providers, and that they have actual knowledge of the infringements). The resulting injunction is a no-fault injunction, which (if transposed to the Australian context) does not depend on a finding of authorisation by the ISP, and stands separate from concepts of extended authorisation liability in that it merely seeks to provide an efficient response to clear, commercial-scale infringements that are based overseas. The rightsholders are responsible for initiating the action, the Court reviews the evidence and supervises the process and the granting of an injunction (including its terms), and the ISP then complies with the injunction.

Although Australia does not have an equivalent of Art 8(3) of the Information Directive or the Enforcement Directive, they provide strong support for the policy direction indicated in the Discussion Paper. A provision based around the UK s97A with some modification would provide the necessary no-fault jurisdiction for a Court to make a site blocking order. Despite having missed previous opportunities to bring Australia into line with the level of protections available under EU law, the introduction of a no fault extended injunction would put Australia on an equal footing with its European counterparts, including the United Kingdom.

Australia would not be the only country in the region to embrace a site blocking law. Singapore’s parliament has recently enacted a site blocking law, mirroring the United Kingdom’s 97A (Copyright (Amendment) Act 2014, s 6 ff) that now awaits Presidential Assent. It followed an earlier recommendation by the Media Convergence Review Panel, which deemed site blocking one of the most appropriate responses online infringement (the other two being public education and availability of legitimate digital content). The Media Convergence Review Panel was co-chaired by a representative of an intermediary.

Effectiveness and proportionality

Site blocking injunctions are effective. The fact that some subscribers (likely to be a small minority) could seek to circumvent the orders does not deny their effectiveness (indeed, such circumvention requires considerable technical skill and patience). In the BT case, Arnold J considered a challenge to the efficacy of the site blocking orders by an ISP claiming that subscribers could circumvent the orders by several technical means. Arnold rejected the challenge and made the site blocking order, finding that it was justified even if it only prevented access by “a minority of users”.

---

66 Google’s Head of Policy & Government Affairs, Southeast Asia was the co-chair of the Media Convergence Review subcommittee.
67 BT case at [192]ff.
68 BT case at [198].
Later in *EMI Records v BskyB*, Arnold J considered it highly relevant that:  

“… the evidence indicates that blocking orders are reasonably effective. The effect of the order made in Italy with regard to TPB referred to in 20C Fox v BT at [197] was a 73% reduction in audience accessing TPB in Italy and a 96% reduction in page views. The blocking order made in Italy in relation to KAT has had a similar effect. As for the effect of the orders made in England in relation to TPB, as at 19 December 2011, TPB was ranked by Alexa as number 43 in the UK, while as at 21 November 2012, its UK ranking had dropped to number 293.”

Following these earlier orders against Newzbin (2011) and The Pirate Bay (2012), in 2013 a High Court of Justice (Chancery Division) decision resulted in more than 25 site blocking orders issued over a 9 month period. The orders applied to the top six ISPs in the U.K., constituting the majority of the home internet market in the U.K. Recent research comparing site visits in February 2014 to one month prior to each of the site blocks found that visits to all of the blocked sites declined by more than 90%. Comparing combined visits to the blocked sites and proxy sites providing access to those sites prior to and after the 2013 waves of blocking, visits were down 86% in February 2014.

Similarly, comparing Alexa data on page views in June 2014 to one month prior to each of the site blocks, page views to all the blocked sites declined more than 73%. Focusing on five popular blocked sites, ThePirateBay, Kickass, Vodly, Movie4k, and Primewire, page views decreased more than 95% in June 2014, compared to one month prior to each of the site blocks.

With specific reference to proportionality, the Court of Justice of the European Union (being the highest appellate Court in the European Union, whose decisions are binding across all EU Member States) ruled in the *Kino* case that the blocking order does not need to lead to a complete cessation of the infringement and acknowledged that blocking orders are inherently capable of being circumvented, as long as it discourages users from accessing the file and is:  

“… sufficiently effective to ensure genuine protection of the fundamental right at issue, that is to say that they must have the effect of preventing unauthorised access to the protected subject-matter or, at least, of making it difficult to achieve and of seriously discouraging internet users who are using the services of the addressee of that injunction from accessing the subject-matter made available to them in breach of that fundamental right.”

In the BT case, Arnold J rejected an argument by the ISP that the form of order was not proportionate, instead finding that “The order is a narrow and targeted one, and it contains safeguards in the event of any change of circumstances. The cost of implementation to BT would be modest and proportionate.” Similarly, in *Paramount v BSkyB*, Henderson J found that a site blocking order was proportionate bearing in mind the nature of the website in question, the likelihood that affected internet users would

---

69 *EMI Records v BskyB* [2013] EWHC (Ch).
70 at [106].
71 See Annexure A – MPA Analysis of Alexa and ComScore Data - “Impact of Third Party Orders on Traffic to Infringing Sites”
72 *Kino* (UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft mbH (Case C-314-12, 27 March 2014) (*Kino*) at [64].
73 at [200].
know it was infringing and that legitimate content was available elsewhere and users would not be derived of it.74

93 In the Kino case, the CJEU (being the highest appellate Court in the European Union, whose decisions are binding across all EU Member States) found that the site blocking orders were proportionate because the orders allowed the ISP to determine the precise means of implementation to achieve the objective, they did not “unnecessarily deprive internet users of access” to legitimate content and the measures had the effect of preventing “or at least making it difficult to achieve and of seriously discouraging internet users who are using the services of the addressee of that injunction from accessing the [infringing] subject-matter.”75 While the Netherlands Court of Appeal reached a different conclusion in Stichting BREIN v Ziggo B.V. & XS4All Internet B.V. (Ziggo case), this decision (which is currently on appeal to the CJEU) was handed down prior to the CJEU’s judgment in the Kino case. Accordingly, given that the CJEU’s judgments are binding on the courts of all European Member States, the Netherlands Court of Appeal’s decision in the Ziggo case is expected to be reversed. The CJEU are expected to find instead that, in line with the Kino case, the blocking orders in the Ziggo case are not inappropriate, even though they may technically be circumvented, including because not all users will attempt or be able to circumvent them and because blocking has an educational value in informing users of the illegality of the site.

94 One consideration in terms of the proportionality of a site blocking order is whether it results in over-blocking of websites – unintended restrictions of other non-infringing material. The risk of over-blocking primarily exists when other websites are located on the same server as the piracy website intended to be blocked. The UK film and music industry ensure that piracy sites referred to the courts for blocking orders have either 1 or more dedicated IP addresses for their sole use. In the instance when an IP address(es) resolves to more than one site, the onus of due diligence is on the rights holder to ensure the IP addresses they provide to the court are correct and do not impact other sites. This always been satisfied in the United Kingdom. There has only been one case where one site (TorrentFreak.com) was inadvertently blocked when the court issued blocking orders against piracy website EZTV. However that only occurred as a result of deliberate action by EZTV who modified their DNS entries after being blocked to have the same IP address as that of the ‘Torrent Freak’ website resulting in said online publication being blocked as well.76

Costs and other considerations

95 The fact that costs will be incurred by the ISP is not a ground for refusing a site blocking order under European law. In the BT case, Arnold J was prepared to make site blocking orders even though implementing them may represent significant costs, have considerable organisational impact and require difficult and complex technical solutions within the ISPs business. In Paramount v BSkyB, one

74 Paramount v BSkyB at [42].
75 Kino at [64].
of the most recent site blocking decisions, Henderson J went further and held that “the cost of compliance will, therefore, be relatively modest and will not cause them any particular difficulty.”

In the *Kino* case, the CJEU held that since the ISP is not required to make “unbearable sacrifices”, that the costs were not disproportionate to the benefits the injunction was designed to achieve in protection of the rights of rightsholders. This decision is now binding on all EU Member States.

Attempts have been made in Europe to argue that site blocking injunctions interfere with fundamental rights and the freedom of expression under Article 10 of European Convention on Human Rights (ECHR). However, these arguments have been consistently rejected. The CJEU has confirmed that third party injunctions against ISPs made under these laws are consistent with the “fundamental rights recognised by EU law”. These were considered to include the “freedom to operate a business” and the “freedom of information of internet users”.

In *Kino*, the CJEU found that a site blocking injunction did not infringe “the very substance of the freedom of an internet service provider”. This is because it leaves the ISP to determine the specific measures to be taken to achieve the result – which can involve the use of measures “best adapted to the resources and abilities” of the business - and it is sufficient that the ISP takes reasonable measures to achieve the objective. The CJEU concluded that:

“...the fundamental rights recognised by EU law must be interpreted as not precluding a court injunction prohibiting an internet service provider from allowing its customers access to a website placing protected subject-matter online without the agreement of the rightholders when that injunction does not specify the measures which that access provider must take and when that access provider can avoid incurring coercive penalties for breach of that injunction by showing that it has taken all reasonable measures, provided that (i) the measures taken do not unnecessarily deprive internet users of the possibility of lawfully accessing the information available and (ii) that those measures have the effect of preventing unauthorised access to the protected subject-matter or, at least, of making it difficult to achieve and of seriously discouraging internet users who are using the services of the addressee of that injunction from accessing the subject-matter that has been made available to them in breach of the intellectual property right, that being a matter for the national authorities and courts to establish.”

Courts in the United Kingdom have reached the same conclusions. One of the clearest statements of this position is found in *Paramount v BSkyB*, with Henderson J ruling that the site blocking order being sought would not interfere with fundamental rights of customers under the ECHR:

“It appears to me plain that the result of the balancing exercise is that the rights of the Applicants to protection of their copyright should prevail over the rights to freedom of expression and other rights of the other groups of persons whom I have mentioned. The operators of the Target Websites appear to be involved in an activity which they must know is wholly illegitimate. So far as the users of the Target Websites are concerned, they must also for the

---

77 *Kino* at [51]-[53].
78 See e.g. *Kino* at [47].
79 *Kino* at [52].
80 *Kino* at [53].
81 *Kino* at [64].
82 *Paramount v BSkyB* at [42].
This reasoning would strongly support the introduction of no-fault site blocking orders in Australia. Sites like Pirate Bay and the range of torrent and P2P sites that have been blocked in the United Kingdom are all primarily infringing sites, which would be apparent to consumers and are offering content that could be obtained legally in Australia – usually from a variety of channels. Recent research indicates that almost 50% of Australian adults believe that Australian courts should be allowed to decide to block overseas websites that solely profit from pirated movies, TV shows or other copyrighted content. 63

Compliance with Australia’s international obligations

It is clear that targeted site blocking injunctions under s 97A have proven to be an effective, targeted and proportionate response to online copyright infringement. In many cases, they represent the only feasible way of preventing a continuation of infringements that are being deliberately conducted from a foreign site to frustrate local laws and enforcement procedures.

In addition to being in line with international best practice, a provision for extended injunctive relief requiring ISPs to block access to infringing foreign sites would also be compliant with Australia’s international obligations. It would provide the requisite protection of the right of communication to the public under Art. 8 of the WCT, without contravening the agreed statement limiting the scope of relief against service providers (as mirrored by the safe harbour scheme in the AUSFTA).

With the above international precedents for an effective and proportionate course of action against online piracy, the Australian Film/TV Bodies strongly support the intention behind Proposal 2.

A new provision providing for extended injunctive relief could easily be incorporated into the Copyright Act. It is important that this new provision be clearly distinguished from the right to bring an action “for infringement of the copyright” under s 115, to ensure that it stands apart from fault based relief and cannot be classified as a form of relief only available in a traditional case of copyright infringement (as is the case with s 116). For example, it could be enacted as a new s 115A. Specific comments regarding the detail of Proposal 2 are provided in the answer to Question 6 below. The issue of costs is addressed separately in the following section.

QUESTION 6: What matters should the Court consider when determining whether to grant an injunction to block access to a particular website?

The types of matters an Australian Court should take into account when making a site blocking order are similar to the matters that have been taken into account by Courts applying EU law, notably in the UK. The considerations in the UK context as part of the judicial assessment are mandated by the local

63 2014 Sycamore research, to be released in Q3 2014.
implementation of the European Human Rights Act, of whether the site blocking order is proportionate in light of the competing rights of the copyright owners (to protection of their IP) as well as the rights of the operators and users of the target websites (to freedom of expression, privacy and protection of personal data). In all cases to have reached the High Court so far, the requested site blocking orders have passed this test.

106 Like those provisions, and the jurisprudence that has been developed under them, an Australian extended injunctive relief provision should:

(a) be directed to online locations that are operated outside of Australia, which the rightsholders would bear the onus of proving were involved in infringing activity;

(b) allow a number of ISPs to be listed as respondents to an application for an injunction (although it is probably unlikely to be necessary to specifically provide for this in the legislation itself);

(c) involve evidence that the online location infringes copyright, and that the services of the ISPs are used by the operators of and visitors to the site to do that; and

(d) retain the Court’s discretion as to whether an injunction will ultimately be granted – which could involve some of the same considerations as the enquiry.

107 The extended injunctive relief provision should not require the Court to be satisfied that the dominant purpose of the website is to infringe copyright. Raising the level of proof in this way may severely compromise the effectiveness of the new provision in that it would become significantly more difficult for rightsholders to obtain an injunction under the scheme: allegedly non-infringing content would be pointed to in each case, not for reasons of freedom of access to information on the internet, but purely as a basis to defeat the order.

108 Any new extended injunctive relief proposal in Australia would necessarily be subject to the Court’s ultimate discretion as to whether or not an injunction should be granted. This is a fundamental part of the Court’s inherent powers, which would not require specific legislative drafting beyond recognising that the power can be exercised by a Court (e.g. A Court “may”). Given that Australia does not have the same overarching human rights legislation as the UK and the EU, the balancing exercise would be less involved than that reflected in the European and UK cases.

109 Finally, the Australian Film/TV Bodies submit that the new Australian site blocking provision should reflect the Irish and Singaporean, and not the UK model, on the issue of ISP knowledge. That is, like Ireland and Singapore, there should be no requirement that service providers have actual knowledge of infringements. This would be consistent with the ‘no fault’ character of the provision, and the evidentiary burden on copyright owners to prove that the website is being used to infringe copyright,

and the ISP’s services are being used to achieve this. It is an important adjustment to the balance
struck in the UK which reflects the absence of the full proportionality exercise when s 97A is
transposed into Australian law.

110 The proposal that rights holders be required to meet any reasonable costs associated with an ISP
giving effect to an order and to indemnify the ISP against any damages claimed by a third party is
disproportionate, unnecessary, out of step with international practice and contrary to the fundamental
principles of copyright law.

111 As discussed at paragraphs 92 and 95 above, the UK cases have demonstrated that the costs of
complying with an injunctive relief order are not excessive, and that ISPs can deploy existing
technology that they are already using to do so. Indeed, in the second judgment in the BT case
(dealing with the precise form of relief to be granted: [2011] EWHC 2714 (Ch)), Arnold J found that:

“the cost to BT “would be modest and proportionate” is supported by the evidence subsequently
filed by BT, which estimates the initial cost of implementation at about GBP 5,000 and GBP 100
for each subsequent notification.”

112 For these reasons, courts have ordered the costs of site blocking injunctions be borne by the ISP. The
Australian Film/TV Bodies submit that the same position should be adopted in Australia, especially as
it is not likely that the evidence would be any different on a similar application here.

113 An extended injunction provision would also preclude claims by third parties against ISPs that
implement Court-ordered site blocking. This would negate any need to consider indemnification as
part of the new extended injunctive relief provision. To introduce a requirement for indemnification
would unnecessarily fetter the existing powers of the Australian Courts and be inconsistent with
international site blocking laws and decisions in EU member states. In the second judgment in the BT
case (referred to in paragraph 111 above), Arnold J found that:

“In my view there is no reason to require the Studios to give a cross-undertaking in damages.
There is no analogy between an order under Article 8(3) and an interim injunction. An interim
injunction is granted before the parties’ legal rights and liabilities have been ascertained. The
original and main purpose of the crossundertaking in damages was and remains to attempt to
protect the party enjoined if it subsequently transpires that no injunction should have been
granted because the party applying for the injunction did not have the rights claimed or they
were not infringed or for some other reason: see Griffith v Blake (1884) 27 ChD 474 and F.
Hoffmann-La Roche & Co Ag v Secretary of State for Trade and Industry [1975] AC 295 at 360-
361 (Lord Diplock). By contrast, final injunctions are not subject to cross-undertakings (except
sometimes pending appeal). An order under Article 8(3) is a final injunction, and accordingly
there is no warrant for a cross-undertaking”.

5 Extended safe harbour scheme

Proposal 3—Extended safe harbour scheme

\(^{65}\) (at [32]-[33]).
\(^{66}\) (at 34-52 )
The Copyright Act would be amended to extend the application of the safe harbour scheme to entities engaged in the activities set out in sections 116AC to 116AF. This would be achieved by removing the reference to carriage service provider and replacing it with a definition of ‘service provider’, being any person who engages in activities defined in sections 116AC to 116AF.

114 The Australian Film/TV Bodies do not support an extension of the safe harbour provisions under Div 2AA of the Copyright Act unless it is part of a range of other amendments being made to the safe harbour scheme and there is an extension being part of a package of amendments to authorisation liability and to injunctive relief, as described above.

**The current scheme**

115 The safe harbour scheme was introduced into the Copyright Act with effect from 1 January 2005. As described above (paragraph 22), the introduction of the Australian safe harbour scheme followed the successful conclusion of the AUSFTA.

116 Article 17.11.29 of the AUSFTA requires each party to include legal incentives in their respective domestic legislation that would encourage service providers to cooperate with copyright owners in deterring the unauthorised storage and transmission of copyright protected materials. In exchange for this cooperation, service providers receive the benefit of limitations in relation to the scope of remedies available against them for copyright infringements that they do not “control, initiate, or direct” that take place through systems or networks controlled or operated by them or on their behalf.

117 The safe harbours were last elements of the package of provisions, beginning with the DAA, to put Australia at the “cutting edge of online copyright reform”. The practical effect of the scheme is that ISPs that are exposed to authorisation liability and need protection from the full extent of remedies available to copyright owners in the event that they are found to have authorised – non-monetary remedies such as damages and accounts of profits, together with non-monetary remedies such as injunctions. It responds only if authorisation liability is found against the ISP.

118 The safe harbours were introduced to ensure that Australia complied with its obligations under the AUSFTA. It has never been doubted that the existing scheme, limited to ISPs, is fully compliant with Australia’s obligations under the AUSFTA. Any change to the safe harbours is not, therefore, needed to ensure that Australia is compliant with its international treaty obligations (unlike the changes needed in relation to authorisation liability under s101 and s112E described above).

119 Although the term “service provider” was not defined in the AUSFTA, a conscious decision was made by the government in Australia to implement the safe harbours for the benefit of ISPs only. A previous Consultation Paper regarding this issue noted that the definition of “carriage service provider” was chosen because it “was adopted from the Telecommunications Act (the TA) because it was

---

87 Part V Division 2AA of the Copyright Act 1968 (Cth).
88 ISP would remain liable for infringements that they did “control, initiate, or direct”.
90 Second Reading Speech of the Attorney-General (Darryl Williams), see above paragraph 20.
considered to be a suitable and technologically neutral term”. However no reference was made in the Explanatory Memorandum to the US Free Trade Agreement Implementation Bill 2004 to entities other than ISPs obtaining the benefit of the Australian scheme. This is in keeping with the stated purpose of the Australian scheme, which is set out in s116AA of the Copyright Act, namely “to limit the remedies that are available against carriage service providers for infringement of copyright that relate to the carrying out of certain online activities by carriage service providers.”

The term carriage service provider is defined in s10 of the Copyright Act as having “the same meaning as in the Telecommunications Act 1997.” Section 87 of the TA defines carriage service providers as those entities who satisfy a number of requirements including the provision of a service to the public for communications between a point in Australia and one or more other points using a link provided by a licensed carrier. Under s128 of the Telecommunications (Consumer Protection and Service Standards) Act 1999, a CSP must enter into a Telecommunications Industry Ombudsman (TIO) scheme and this information is published and searchable by members of the public. In effect, a carriage service provider is a regulated entity in Australia.

The existing scheme has been judicially considered on only two occasions: in the Cooper case and the iiNet decision, both involving ISPs. In both instances the ISPs were found not to have met the requirements for the scheme, primarily because the ISPs in each case failed to meet the requirement that they “adopt and implement a policy of terminating the accounts of repeat infringers, in appropriate circumstances” under s116AH.

Deficiencies in the current safe harbour scheme

As the result in the iiNet decision highlights, the current safe harbour scheme is deficient in a number of respects that require more urgent attention.

After the iiNet decision the scheme has become largely irrelevant under Australian copyright law. The scheme is redundant in circumstances where, as occurred in iiNet, an ISP is not exposed to liability for authorisation by doing nothing in the face of proven infringements of copyright on its network. The ISP in iiNet avoided liability based on complete inaction even though that inaction denied it the benefit of the safe harbour defences. It never needed to call on the safe harbours. Instead of the scheme providing incentives for ISPs to cooperate, the safe harbours have not created any incentives for cooperation and no cooperation has resulted. Unless there is a risk of liability for authorisation in the first place, an ISP would never need to call on the safe harbours and they would remain irrelevant and fail to fulfil their intended purpose under the AUSFTA.

91 Attorney General’s Department, Consultation Paper, “Revising the Scope of the Safe Harbour Scheme” (October 2011), p 3.
92 Circulated by the Hon Mark Vaile MP, Minister for Trade
93 Note Chapter 16 of the AUSFTA Report No. 61 by the Joint Standing Committee on Treaties also supports the Australian Film/TV Bodies’ view, with the relevant part of the report dealing with the Australian Scheme titled “Internet Service Provider (ISP) Liability”. No reference is made to service providers who are not also ISPs.
The detailed requirements of the safe harbours also require amendment to bring them into line with the practices under international schemes (referred to above in paragraphs 30 and 32). Currently, the main operative obligation on an ISP under the safe harbours is to “reasonably implement” a policy in relation to the accounts of repeat infringers, which is inflexible.\(^95\) The only requirement of such a policy is that it provides for the “termination of the accounts of repeat infringers”.

The Australian Film/TV Bodies do not call for the termination of accounts. Other responses (as described in section 3 above) are more appropriate and modern approaches to minimising online copyright infringements. By limiting the existing requirement to “termination”, the safe harbours arguably provide no protection for an ISP that is seeking to cooperate with rights holders and implements a procedure which involves warnings or throttling of the speed of an internet service. This modernisation of the trigger requirements is appropriate to bring the safe harbours into line with current international practice – such as under the voluntary scheme in the US, discussed above.

Modifying the requirement around the policy to include other more flexible responses to infringement would not put Australia in breach of its obligations under the AUSFTA. Australia is obliged to offer “protections … no less generous” than those available under US law. The introduction of lesser required action, the choice between which is at the election of the ISP, would offer greater not lesser protections for ISPs under Australian law.

Another important omission from the Australian safe harbour scheme is the administrative subpoena process available to copyright owners under the US safe harbours to facilitate the expeditious access to contact details of a subscriber suspected of engaging in copyright infringement without having to commence substantive proceedings to do so.\(^96\) A rights holder is not required to pay a fee (other than to the Court issuing the subpoena) or provide an indemnity for the ISPs costs involved in disclosing a subscriber’s details. The subpoena process was a key element in the balance struck by legislators between the rights of copyright owners and the rights of service providers, including ISPs and is integral to the safe harbour framework.

Australia did not adopt such a subpoena regime, despite the terms of Article 17.11(29)(xi).\(^97\) The explanation for not doing so was said to be the availability of existing Court based processes, such as an application for preliminary or pre-trial discovery under the Federal Court Rules (now known as Div 7.3). This was not a good policy outcome at the time. No sensible comparison could be made between the expeditious process of applying to a Registrar for the issuing of a subpoena and the lengthy, costly and procedurally complex process of applying to a judge for an order for preliminary or pre-trial discovery, which may be contested. An ISP that claims to comply with the requirements of the safe harbours could refuse to consent to preliminary or pre-trial discovery production; Australian ISPs have already done so. There is no reason to expect that other service providers are likely to do the same.

\(^95\) Copyright Act, s 116AH.
\(^96\) See section 512(h) of the U.S. DMCA.
\(^97\) Which provides that “Each Party shall provide for an administrative or judicial procedure enabling copyright owners who have given effective notification of claimed infringement to obtain expeditiously from a service provider information in its possession identifying the alleged infringer.”
Deficiencies in Proposal 3 – Extended safe harbour scheme

129 The Discussion Paper does not contain a detailed explanation why it is necessary or appropriate for the safe harbours to be extended to cover universities and search engines. One of the reasons suggested for the need for change is a potential problem around the use of the phrase “to the public” and whether this excludes institutions such as universities. This is a weak ground for change. There is no doubt under Australian copyright law that the phrase “to the public” has been interpreted broadly to mean persons other than in a private capacity. It is sufficient if they could be members of the copyright owners’ public, as the decisions of the Full Court in Cooper and iiNet and of the single judge in Kazaa demonstrate.98

130 Calls for an extension to the scheme to non ISP service providers are not new. However, calls for legislative change have been made on the basis of a theoretical concern about the risks to which non ISP service providers could be exposed without the benefit of the safe harbour. The theoretical basis for such risks is weak. Before the safe harbours are engaged, there would need to be a finding of authorisation liability.

131 There is also no empirical evidence supporting the need to extend the safe harbours beyond ISPs. There is no evidence, let alone any experience under Australian law, where such a service provider has been the subject of any copyright claim or had been exposed to any liability in Australia because it was unable to rely on safe harbours in defence of any remedies. There is similarly no evidence that these service providers have needed to invoke the benefit of safe harbours in other countries to mitigate their exposure in other countries with the same safe harbour scheme – such as the US.

132 Care needs to be taken in making comparisons between the Australian safe harbour scheme and those of other countries, such as the US and Korea:

(a) Under US law there is no statutory recognition of the liability akin to authorisation; the law of contributory and vicarious liability is based solely on common law principles developed by the US Courts from time to time.99 There is no equivalent of “authorisation” under s101 of the Australian Copyright Act, nor is there any equivalent of the mandatory factors under s101(1A) of the Australian Act or the recognition of an industry code in s 101(1A)(c). The US scheme does not have an equivalent provision to s112E which, unlike the safe harbours under US law, is a complete defence to infringement and is not tied to any countervailing obligations on the part of the provider to take steps to assist in enforcement. This defence is not limited to carriage service providers.100 On the other hand there is evidence that a broader safe harbour could be invoked by the operators of services that are involved in copyright infringement, such as content

98 Roadshow Films Pty Ltd v iiNet Ltd (2011) 275 ALR 1 at [341]-[345] and [692]; Universal Music Australia Pty Ltd v Cooper (2005) 150 FCR 1 at [64]-[68]; Kazaa at [420].
100 In Kazaa (Universal Music Australia Pty Ltd v Sharman License Holdings Ltd[2005] FCA 1242) at 395 Wilcox J held that the “qualifying elements” of s112E applied to Sharman, although his Honour subsequently found that there were other factors that disqualified Sharman from reliance on the section.
hubs and cyberlockers, as has occurred under the US safe harbour provisions (e.g. In Re Aimster101, Napster102 and Isohunt103).

(b) Although the definition of online service provider is broader under the Korean copyright law and carriage service provider under the Australia Act, there are far more stringent requirements imposed on service providers under Korean law104 and Korean online service providers may be fined for non-compliance. Korean online service providers must now also register with the Korean Copyright Commission and to obtain and maintain a license they must prove they have “effective filtering systems in place”. The business licence may be cancelled if there are three fines under the copyright laws.

133 Treating all “service providers” as if they were a single type of business ignores and obscures the differences between them. Search engines and educational institutions have very different business models and operational structures. The incentives for cooperation with rights holders may be different in each case, as would be their capacity to meet the pre-conditions for taking the benefit of the safe harbours. A code (such as provided for under 116AH) may be necessary given that there may be little or no utility for such service providers (such as social media networks or email providers) having a policy under 116AH allowing for the termination of repeat infringers which would invariably never be exercised (because of the mixture of services offered to the user) or never be exercised effectively (because of the manner in which the services are offered to the users).

134 The extension of the safe harbours to a wider category of providers necessarily involves a recognition of their capacity to control user activity because they would immediately become subject to the requirement to “adopt and implement a policy of terminating the accounts of repeat infringers, in appropriate circumstances” (s116AH); the take down regime that applies in respect of Category D activities; and the ability of a Court to order termination of the subscriber account or disabling of access to the linked content even if the safe harbour applied. The providers could only be seeking the protection of the scheme if they were ready and willing to exercise control over their users.

135 Given that the existing scheme is compliant with Australia’s obligations under the AUSFTA, the weak basis for seeking an expansion and absence of any empirical evidence for the need for amendment, the Australian Film/TV Bodies urge the government to take a cautious approach to this issue.

101 In Re Aimster 252 F.Supp. 2d 634 (N.D Ill. 2002).
102 A&M Records, Inc v Napster,Inc., 239 F.3d 1004 (9th Cir. 2001).
104 Under the Korean Copyright Act 1989, amended in 2009 to addresses online copyright infringement more broadly, the government may order an online service provider to (1) warn an infringing subscriber; (2) delete or cease transmission of infringing copies; (3) suspend the account of repeat infringers for up to six months; and (4) suspend a bulletin board service for up to six months.
QUESTION 7: Would the proposed definition adequately and appropriately expand the safe harbour scheme?

136 There are a number of problems with the proposal in the Discussion Paper to change the definition of service provider under the existing safe harbour provisions. Replacing the words “carriage service provider” and with the words “service provider” would not be an adequate or effective policy response and the Australian Film/TV Bodies urge the government to reconsider the form of the proposal.

137 The words “service provider” would need to be defined, as they are in the US Copyright Act, on which the Australian safe harbours are based. The words “service provider” is a defined term under s 512 of the US Copyright Act – with two operative definitions, depending on the provisions involved:

“(k) Definitions.—

(1) Service provider.—

(A) As used in subsection (a), the term “service provider” means an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user’s choosing, without modification to the content of the material as sent or received.

(B) As used in this section, other than subsection (a), the term “service provider” means a provider of online services or network access, or the operator of facilities therefor, and includes an entity described in subparagraph (A).”

138 The first of the definitions applies only to transmission or routing activities – equivalent to the current Category A activities under the Div 2AA of the Australian Copyright Act. The second definition, which is more limited, applies to all other types of activities covered by the safe harbours – e.g. linking and hosting services under Categories C and D of the Australia safe harbour regime. Any change to the Australian definition of “carriage service provider” would need to adopt definitions equivalent to those under the US Copyright Act. These different concepts of “service provider” are already reflected in the definition in the AUSFTA, with which Australia is required to comply.105

139 A number of other textual changes would need to be considered, together with substantive changes where there are currently deeming provisions that favour an ISP but which would be more problematic if extended to non-ISP service providers. An example is the definition of “financial benefit” in s116AH, which makes reference to the “industry practice in relation to the charging of services by carriage service providers, including charging based on the level of activity”. Services providers such as P2P operators (MovieX106) and cyberlockers (e.g. equivalents of the US based Hotfile107) could claim that they had a legitimate server space business or search engine functionality that entitled them to safe

---

105 Art. 29 (xi) defines “service provider” as follows: “For the purposes of the function referred to in clause (i)(A), service provider means a provider of transmission, routing, or connections for digital online communications without modification of their content between or among points specified by the user of material of the user’s choosing, and for the purposes of the functions referred to in clause (i)(B) through (D), service provider means a provider or operator of facilities for online services or network access.”


harbour protection; despite the operations being funded by infringement. Similarly, the special presumption of compliance with the scheme in favour of ISPs, set out in s116AI would be inappropriate if it was extended beyond regulated ISPs.

The removal of the definition “carriage service provider” would also effect a significant change to the regulatory framework sitting behind the safe harbours. Removal of the words “carriage service provider” would also involve the removal of the reference to the section 87 of the *Telecommunications Act* and remove the current link between entities that seek the benefit of the safe harbours and regulatory controls over those entities under the *Telecommunications Act* e.g. licence conditions, submission to Codes registered under the *Telecommunications Act*, the TIO complaint handling procedures and regulatory oversight by ACMA. Regulatory oversight is something lacking in relation to non-ISP service providers.

The change would also necessitate changes to the authorisation liability provisions. Given that the safe harbours are initiated only if authorisation is first established, the authorisation provisions would need to be amended to impose liability on the entities that would fall within this extended definition of service providers equivalent to the liability that would be imposed on ISPs. These additional service provider entities would also need to be made subject to any Code or Regulations in place under s101(1A) and the liability if they failed to meet obligations set under a Code or Regulations.

This presents a difficulty because only ISPs can be made liable to comply with Codes which are capable of being registered under the Telecommunications Act 1997. This means that if the safe harbours are extended to service providers beyond those that are regulated, or capable of regulation, by Code under the Telecommunications Act 1997 they would obtain the benefits of minimising their exposure to remedies at the same time as they have a lesser risk of authorisation liability than ISPs, that are subject to a Code under the Telecommunications Act.

There would also need to be amendment to the safe harbour scheme under Div 2AA to introduce a low cost disclosure / subpoena scheme as exists under the DMCA in the United States to overcome the gap situation that current exists (see above paras 127 and 128). There cannot be any serious doubt that such a process is needed to put copyright owners on the same footing in Australia as in the United States - redressing the discriminatory treatment copyright owners current face enforcing their rights in Australia. The costs of bringing preliminary discovery and pre-trial actions increased substantially after the previous government ramped up Court fees facing copyright owners (a decision condemned throughout the legal community and the judiciary). Nor could any Australian ISP raise any sensible objection to the introduction of a procedure that applies to all ISPs in the US market, without any evidence of difficulty or that it has imposed any unreasonable burdens. Further, there is a very strong argument that Australia is, and has been since 2005, in breach of its obligations under the

---

108 Section 116AI states "If a carriage service provider, in an action relating to this Division, point to evidence, as prescribed, that suggests that the carriage service provider has complied with a condition, the court must presume, in the absence of evidence to the contrary, that the carriage service provider has complied with the condition."
AUSFTA because it has failed to implement a subpoena style scheme into the safe harbours. That issue can be resolved now with the introduction of such a scheme into the safe harbours.

**QUESTION 8: How can the impact of any measures to address online copyright infringement best be measured?**

144 The Australian Film/TV Bodies support the need for any response to online infringement to include the measurement and assessment of the impact of measures implemented to address online copyright infringement.

**Building the evidence base**

145 The absence of a commonly accepted approach for quantifying the volume and impact of infringement has posed a challenge to addressing online copyright infringement. It led to questionable research asserting that copyright infringement does not in fact harm legitimate sales.\(^{109}\) It has denied policy makers a reliable basis for testing competing claims about effectiveness/lack of effectiveness of potential measures before they have been tested. Professor Hargreaves observed that “No one doubts that a great deal of copyright piracy is taking place, but reliable data about scale and trends is surprisingly scarce”.\(^{110}\) The absence of agreed methodologies has also enabled assertions to be made that the types of measures described in the Discussion Paper (graduated response schemes and extended injunction schemes) would be ineffective without any evidence to support them.

146 There are signs that this is changing. On 4 July 2014 the Intellectual Property Office of the United Kingdom released a report it commissioned from the University of Hertfordshire, by Callopy and others (the IPO Report).\(^{111}\) The aim of the report was to provide “a robust overview of existing methods used to measure infringement of intellectual property rights (IPR) as well as recommend suitable methodologies, especially those capable of being adopted across different IP rights”. It is one of the few government reports in the field and should be recognised as making a serious attempt to both assess the current evidence of infringement and create a baseline for further research.

147 Importantly, the IPO Report rejected the types of criticisms directed towards rightsholders over their existing research – recognising it to be of the highest standard amongst trade organisations:\(^{112}\)

> “The software, recorded music, motion picture and video trade bodies are responsible for providing the majority of wide-scale online infringement research and, despite criticisms from many commentators, these research reports and their commitment to research quality are in our view of the highest standard amongst the various trade bodies. We also identified a commitment to a wide range of research within this group of trade bodies and a willingness to consider using (if not already doing so) new technological solutions to assess the scale of infringements.”


\(^{112}\) Callopy Report at 60.
Such an approach is also consistent with the IPO Report, which found that:

“Online copyright infringement should be assessed by the blended combination of the number of ‘take-down’ notices, omnibus research of the level of compliant and infringed activity by consumers, and a survey of organisations regarding their evidence of infringement notifications prior to enforcement and their assessment of criteria for a challenge. The use of emerging technological tools to measure observable online behaviour should be added to the blend of approaches to provide a more accurate picture.”

Defining the definition of effectiveness

The definition of effectiveness of a content protection initiative should be defined by the degree to which the goals of the initiative have been met. For example, if the stated goals of the initiative are to (1) educate consumers about the importance of copyright protection and (2) help them find better ways to enjoy digital content, the effectiveness could appropriately be defined as (1) decrease in consumer sharing of copyright infringing files; and (2) increase in consumer accessing of legal digital content – ideally measured relative to a “control” or what they would have been in the absence of the initiative. The latter clause is important because the given metrics may increase or decrease due to other factors; correlation is not causation. Research that best assesses the effectiveness of the initiative should isolate the specific effects of the initiative from other environmental effects.

The data used to measure the effectiveness of the initiative should also correlate to the goals of the initiative, and should measure whether the goals of the initiative have been met. In the case of “supply” focused initiatives, the measures can involve quantifying changes in supply, and also, potentially, corresponding changes in demand. In the case of “demand” focused initiative, the focus would be on changes in demand for infringing content, and/or potentially changes in demand for legal content. In the example above, the data collected could involve the number of consumers sharing infringing files, the number of infringing files shared, bandwidth consumed by infringement, as well as the number of consumers accessing legal digital content, and/or the amount of legal digital content being accessed, or some derivation. Given the ideal is to measure these metrics relative to a “control” or what they would have been in the absence of the initiative, where possible data should be analysed in areas that lend themselves to this comparison, such as pre- and post-implementation data, data for other non-affected but comparable jurisdictions, etc. The nature of this data will depend on the initiative.

The availability of the data, and the ways it could be obtained, will be highly dependent on the nature of the metrics being tracked. By its nature, illicit behaviour is often hard to measure, but various approaches can be employed including surveys, panel measurement, direct measurement in some cases, and sampling techniques. Standard statistical and econometric techniques can then be performed to analyse the data. When evaluating measurement studies, the nature and quality of the available data should be assessed. The evaluator should solicit comments and input from industry and other subject matter experts regarding the accuracy and thoroughness of these studies.

---

113 IPO Report, Executive Summary, p 3.
The main impediments in general tend to be the availability of data and the existence of the necessary conditions in the market to isolate the effects of the initiative in question (i.e. a randomized or a natural experiment). Where there are a number of different initiatives and conditions affecting the studied universe, identifying the causal effects of a particular initiative can be challenging and an imperfect process.

**QUESTION 9: Are there alternative measures to reduce online copyright infringement that may be more effective?**

The Australian Film/TV Bodies are very supportive of the proposals made in the Discussion Paper, subject to the comments and suggestions made in this submission, and consider that these proposals (as modified) are the most effective steps that can be taken to reduce online copyright infringement in the current legal, economic and technical environment.

There are no alternative models of measures to reduce online copyright infringement that have gained any level of acceptance internationally. Although private copying levies, which are in place in some European countries, are often raised as a possible “solution” to online infringement, in reality, levy regimes are an anachronism in the internet age, amount to little more than a compulsory licensing regime, and do little to restore the integrity of copyright owners’ exclusive rights. Moreover, they do little to improve public understanding of, and respect for, copyright law and the creative expression that it supports. Still, because private copying regimes and associated levies are raised with such frequency, they and are briefly addressed in the following paragraphs.  

Private copying levies are an out-dated, inefficient and ineffective way of compensating rights holders for online piracy. They were designed for an analogue world, where a levy could be applied to physical recording media such as blank tapes to compensate rights holders for consumers making copies of legitimately acquired media such as an over-the-air TV broadcast (i.e., even in the analogue era, they were never intended to compensate rights holders for true piracy). In a world involving the internet, and a world where the purpose of private copy levies would be expanded to compensate not only for traditional private copying but also for piracy, the only way that a levy could work is to attach it to the internet service or to the devices capable of connecting to the internet, and to raise the level of the levy substantially to cover the use of services or devices for piracy purposes. However, levies have not been applied to internet services anywhere in the world.

In the case of devices, the experience of a levy in Europe is not positive. These private copying levies are typically imposed on recording devices and media, which have to be paid whether or not they are used for private copying or piracy. French consumers, pay a levy of €15 on top of the price of an MP3 player. However this leaves open other devices increasingly used to access the content e.g. computers, smart phones and tablets. The Danish Government’s attempt to impose a levy on mobile phone memory cards is currently being challenged in the European Court of Justice (Copydan case).

---

The European Commission’s recent report on copyright reform revealed a significant dissatisfaction with the EU levy regime amongst all stakeholders.115

As indicated above, there are real concerns about whether a levy can even be considered an anti-piracy measure, given the recent decision of the European Court of Justice in the ACI Adam case to strike down a levy that did not discriminate between legal and illegal private copies. In that case the Advocate General delivered an opinion that downloading infringing files from infringing sources would not amount to private copying or be compatible with the copyright treaties. (The Dutch government argued it was to increase its collections of a copying levy).116

A private copying levy was recently rejected by the UK government. The UK, which is a much more relevant comparator for Australia, has recently introduced a new private copying exception that, notwithstanding a slew of other infirmities resulting in significant harm to rightsholders, soundly rejects the application of private copying levies. The responsible Minister, Baroness Neville Rolfe, explained in the House of Lords on 29 July 2014 that “[t]he Government do not believe that British consumers would tolerate private copying levies. They are inefficient, bureaucratic and unfair, and disadvantage people who pay for content.”117 The same reasoning applies in Australia. Applying a levy would impede legitimate services, by taking away the rationale for consumers to pay for legitimate services when a levy will be applied to their internet service anyway.

Further, a levy is likely to be unconstitutional in Australia. In 1993, an amendment to the Copyright Act to impose a levy on vendors of blank tapes was held to be unconstitutional by the High Court. As the levy was a tax, the amendment imposing it was in breach of the “anti-tacking” provision of the Constitution (which prevents Parliament from tacking something else onto a law imposing taxation, or conversely tacking the imposition of a tax onto a law dealing with something else). A new levy imposed in relation to the internet service would suffer a similar fate as the blank tape royalty. These are strong grounds for the Government rejecting any proposal for private copying levies in this country, whether instead of, or in addition to, the proposals outlined in the Discussion Paper.

**QUESTION 10: What regulatory impacts will the proposals have on you or your organisation?**

The Australian Film/TV Bodies understand that the proposals will be subject to the governments’ Regulatory Burden Measurement Framework in accordance with the Australian Government Guide to Regulation published by the Office of Best Practice Regulation (OBPR).

The Australian Film/TV Bodies expect to be heavily involved in implementing and acting on the proposals once they are finalised, including by:

(a) taking steps to finalise an industry code regarding reasonable steps to be taken by ISPs to avoid authorisation liability;

116 It was opposed by the Spanish, Italian and Lithuanian governments and the EU Commission.
117 See the Hansard report at: http://www.publications.parliament.uk/pa/id201415/Idhansrd/text/140729-0001.htm#14072947000224
(b) providing notifications of infringements under, and otherwise complying with, such a code (or regulatory/legislative scheme if required); and

(c) making applications for site blocking orders under the new extended injunctive relief provision of the Copyright Act.

Given the role that these proposals will play in supporting the contribution of the Australian film and television industry to the broader Australian economy and culture by addressing online piracy, the Australian Film/TV Bodies would be prepared to take these steps.

**QUESTION 11: Do the proposals have unintended implications, or create additional burdens for entities other than rights holders and ISPs?**

163 Question 11 is framed as a negative enquiry, whereas it should be framed as a balanced enquiry that calls for both an examination of benefits as well as burdens (if any) of the proposals in the Discussion Paper. There are clearly a range of benefits to other organisations and people from the reduction in online infringement in Australia.

164 There are numerous organisations involved in the supply chains for legitimate copyright material that are currently adversely affected by the unconstrained levels of infringement occurring in Australia. They include all the organisations and their employees involved in the production, distribution, broadcast and screening of film, television and video content.

165 There are also benefits for consumers resulting from bringing online infringement under control. Currently, consumers who purchase legitimate content are subsidising the internet users who take illegally, because it is only the former that are contributing to creation and investment in that content – the latter are free-riding. The legislative changes proposed in the Discussion Paper would provide greater incentives for investment in the creative industries – made in the knowledge of more certain returns – which would lead to greater choice of content being made available for consumers.

166 There is also strong evidence of a correlation between unauthorised sources of content files and other unsafe online activities – including viruses, phishing and identity theft – which often provides the return for suppliers of infringing material. This malware is also found to be embedded in the advertising on these sites which provide the financial returns to the website operators.

167 Recent research by the University of Ballarat explored the relationship between piracy sites and online advertising, which specifically targets Australian consumers, and found that 99% of the advertisements were in the “High Risk” category, categorised by the researcher as being either: sex industry, malware, gambling, scams and downloading adverts. The research found that only 1% of the advertisements on the piracy websites surveyed were “mainstream ads”, in other words advertisements placed by legitimate businesses that operate within the formal economy.

The results of this research found that 46% of the advertisements displayed on these sites were malware: 3% were categorised as unregulated and unlicensed gambling promotions; 20% were sex industry related adverts, exposing pre-teen and teen users who access these websites to pornographic imagery as well as being one click away from hard core pornographic websites. The prevalence of high-risk advertising on piracy sites was corroborated in recently published research commissioned by the Intellectual Property Awareness Foundation (IPAF) into the online habits of 12-17 year olds which found that the most commonly viewed advertisements when accessing piracy sites, according to pre-teens and teens, were sex industry and gambling advertisements.¹¹⁹

The Ballarat research was reviewed by an Executive Board member of the UK Council on Child Internet Safety, the British Government's principal advisory body for online safety and security for children and young people and concluded:

“These data rather blow a hole in the carefully nurtured image of piracy sites somehow being a modern version of Robin Hood. They ain’t. Quite the opposite. If ever it was in any doubt, by accepting advertising from these dubious sources their owners are showing that their snouts are well and truly in the sort of money trough no respectable or ethical business would go near in a million years……Parents who hitherto may not have bothered much about their children’s engagement with piracy need to know about this aspect, about what else their children might be tangling with. Right now I’m afraid largely they don’t. The wider public also need to know more about the reality of piracy. That might help strip away some of the well-honed myths the pirates have spun around themselves.”¹²⁰

Providing incentives to consumers acquire legitimate content and discouraging access to websites and services that offer infringing content is also likely to contribute to a safer online experience for most consumers and their families.

MPA Analysis of Alexa and ComScore Data – “Impact of Third Party Orders on Traffic to Infringing Sites”
Methodology and terminology are defined in Appendix 1.

United Kingdom

2011-2012

In October 2011, U.K. courts ordered British Telecom (BT) to block access to Usenet indexing site Newzbin.com. Following subsequent court orders, other ISPs also implemented blocks in the following months. Newzbin attempted to provide methods of circumvention, and switched to a new URL in February 2012 (Newzbin2.es), which was also blocked.

According to analysis by NetNames, twelve months after the blocking began, despite changing its domain name, Newzbin had lost two-thirds of its reach. In late November 2012, the site’s operator decided to shut down.

In April 2012, U.K. courts ordered ISPs to block access to P2P indexing site The Pirate Bay. In May and June, major ISPs implemented the block. TPB, a highly popular site in U.K., immediately decreased in Alexa ranking. According to Alexa the average rank for TPB in the U.K. was 44 from February 2012 through April 2012, but after the block in May and June 2012, the average rank dropped to a low of 394 during the week of July 29, 2012. Following that point, the Alexa ranking initially increased, but started dropping again in December 2012. In January 2013, the average Alexa ranking was 365.
Following earlier orders against Newzbin (2011) and The Pirate Bay (2012), in 2013 a High Court of Justice Chancery Division decision resulted in more than 25 site blocking orders issued over a 9 month period, grouped below for analysis into three waves. The orders apply to the top six ISPs in the U.K., constituting the majority of the home internet market in the U.K.

Comparing site visits in February 2014 to one month prior to each of the site blocks, visits to all of the blocked sites\(^1\) declined by more than 90%.

Comparing combined visits to the blocked sites and proxy sites providing access to those sites\(^2\) prior to and after the 2013 waves of blocking, visits were down 86% in February 2014.

Full list of sites is available in Appendix 2. This analysis focuses on dedicated and multi-site proxies, which search traffic in the wake of site blocking in U.K. suggests is likely the most sought after workaround in U.K. These sites offer access to a specific site or multiple blocked sites. General VPNs or other proxy services were not included in this study given that the impact is more diffused in that dataset.
Similarly, comparing Alexa page views in June 2014 to one month prior to each of the site blocks, page views to all the blocked sites declined more than 73%.

Focusing on five popular blocked sites, ThePirateBay, Kickass, Vodly, Movie4k, and Primewire decreased more than 95% in June 2014, compared to one month prior to each of the site blocks.
Belgium

In an August 2013 extension to an earlier court order against ThePirateBay (2011), Belgian ISPs were ordered to expand the blocking to include an additional ten torrent websites (listed below) and their domain aliases.

The actions were followed by a significant drop in visits to those sites, evidenced in comScore data. Note that while Kat.ph is blocked, Kickasstorrent’s new domain Kickass.to is not. Nonetheless, visits to Kickass.to (formerly Kat.ph) are down 65% in December 2013 compared to August 2013, according to comScore data.

Belgium: Visits to Blocked Infringing Sites
(Analysis of comScore Media Metrix Data)

Note: When KAT.ph changed its domain name in June 2013, comScore was unable to capture data, so an average of the prior and following month was used. In 2013 ThePirateBay’s domain name changed 9 times, causing fluctuations in visitor levels.
Italy
2011-2012

In April 2011, Italian courts ordered local ISPs to block access to P2P indexing website BTjunkie. In May 2011, the earliest Alexa data available for analysis, BTjunkie ranked at 252 in Italy according to Alexa. By June 2011 the ranking had dropped to 1,555, with an average of 2,464 over the period leading through February 2012, when BTjunkie voluntarily shut down after MegaUpload’s closure.

Similarly, ISPs blocked access to P2P indexing website KAT.ph in May 2012, followed by a major decrease in Alexa page views. In June 2013, Kat.ph changed its domain name to Kickass.to, and within several months, page views were on the rise. However on February 2014, their new domain Kickass.to was blocked, and page views declined again.
2012-2014

Criminal or regulatory orders have resulted in blocking of numerous Bittorrent sites, direct download cyberlocker linking sites, and video streaming web sites in Italy, including waves in April 2013 (hosting/linking) and October 2013 (torrent sites). Between April 2013 and June 2014, criminal or regulatory orders resulted in blocking of over 100 infringing sites in Italy. These actions were followed by a drop in visits to the blocked infringing sites.

The graph below displays trends in Italian visits to 32 out of 112 blocked sites for which comScore data is available\(^3\), not including sites blocked in July 2014. Note that comScore started providing data for Cineblog01 in March 2013 (over 5 million visits) causing the spike, but the site was blocked in April 2013.

The graph below displays page view trends for 39 out of the 112 blocked sites for which Alexa data is available\(^4\), not including sites blocked in July 2014. There was a spike in December 2013 due to ThePirateBay’s (TPB) domain name change; however, the orders had a clear impact in reducing page views to the blocked infringing sites, which is displayed more clearly in the second chart excluding TPB.

---

\(^3\) Full list of sites is available in Appendix 2.

\(^4\) Full list of sites is available in Appendix 2.
Malaysia
On May 30, 2011 Malaysian regulatory body MCMC issued a memorandum to Malaysian ISPs instructing them to block access to 10 copyright infringing websites. By June 17, 2011, all 10 websites were blocked.

The order led to an immediate drop in unique Malaysian visitors to the 10 blocked sites, evidenced in comScore website visitor data. All the sites remained down, and most sites were down more than 70% in January 2012 compared to May 2011.

Malaysia: Unique Visitors to Blocked Infringing Sites
(Analysis of comScore Media Metrix Data)
Netherlands

In early 2012, a regional court ordered Dutch ISPs to block access to ThePirateBay. Blocking ThePirateBay was followed by a significant drop in unique visitors to the sites, evidenced in comScore data. ThePirateBay is down 54% in December 2013, compared to a month before the block (April 2013).

Blocking the site was followed by a drop in page views to the site, evidenced in Alexa data.

5 In late January 2014 ISPs won an appeal and the case is now before the Supreme Court.
Appendix 1: Methodology

**Alexa**

The Alexa data analyzed in this report comprises global traffic data. Alexa computes the reach and number of page views for all sites on the Web on a daily basis based on data collected from millions of Alexa Toolbar users and data obtained from other, diverse traffic data sources.

- The main **Alexa traffic rank** is based on the reach and page view metrics, averaged over time so that the rank of a site reflects both the number of users who visit that site as well as the number of pages on the site viewed by those users.
- **Page views per million** indicates what fraction of all the page views by users go to a particular site. For example, if yahoo.com has 70,000 page views per million, this means that 0.07 or 7% of all page views go to yahoo.com. Since Alexa provides the page views on a daily basis, we are displaying the daily average for that specific month.
- **Reach** measures the number of unique users (visitors). Reach is typically expressed as the percentage of all Internet users who visit a given site.
- **Reach per million** estimates among a sample of one million internet users, how many visited the site on average. For example, if a website’s reach is 12%, 120,000 users visit the site.

**comScore**

comScore maintains an online audience measurement panel with Internet users ages 15+, at home and at work. comScore’s software agent allows a full view of the user experience by recording user activity at the machine or screen-side. For a website to be credited by the agent, the site must be fully downloaded and opened for three seconds. Application use is recorded when it opens at start up, or when the user physically opens it. For online applications, the system can understand who uses a particular application and for how long, but it is not able to determine what is happening inside the application.

- Any person visiting the same website or using the same application more than one time in the same month is only counted once ("unique" visitors).
- **Visits** are the total number of times during a report period that a unique user accessed content within the website with at least a 30 minute (or greater) break in between access times.
Appendix 2: Site Lists

### U.K.: Blocked Sites with comScore Data Available (Page 2)

<table>
<thead>
<tr>
<th>U.K.</th>
<th>Blocked Sites with comScore Data Available (Page 2)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>FILECROP.COM</td>
</tr>
<tr>
<td></td>
<td>TORRENTCRAZY.COM</td>
</tr>
<tr>
<td></td>
<td>TORRENTREACTOR.NET</td>
</tr>
<tr>
<td></td>
<td>KAT.PH</td>
</tr>
<tr>
<td></td>
<td>RAPIDLIBRARY.COM</td>
</tr>
<tr>
<td></td>
<td>EZTV.IT</td>
</tr>
<tr>
<td></td>
<td>TORRENTHOUND.COM</td>
</tr>
<tr>
<td></td>
<td>FILESTUBE.COM</td>
</tr>
<tr>
<td></td>
<td>DL4ALL.COM</td>
</tr>
<tr>
<td></td>
<td>TORRENTZ.COM</td>
</tr>
<tr>
<td></td>
<td>BITSNOOP.COM</td>
</tr>
<tr>
<td></td>
<td>SOLARMOVIE.SO</td>
</tr>
<tr>
<td></td>
<td>TORRENTZ.EU</td>
</tr>
<tr>
<td></td>
<td>THEPIRATEBAY.SX</td>
</tr>
<tr>
<td></td>
<td>1337X.ORG</td>
</tr>
<tr>
<td></td>
<td>TUBEPLUS.ME</td>
</tr>
<tr>
<td></td>
<td>EXTRATORRENT.COM</td>
</tr>
<tr>
<td></td>
<td>KICKASS.TO</td>
</tr>
<tr>
<td></td>
<td>MONOVA.ORG</td>
</tr>
<tr>
<td></td>
<td>1CHANNEL.CH</td>
</tr>
<tr>
<td></td>
<td>THEPIRATEBAY.SE</td>
</tr>
<tr>
<td></td>
<td>FENOPY.SE</td>
</tr>
<tr>
<td></td>
<td>H33T.COM</td>
</tr>
<tr>
<td></td>
<td>MOVIE2K.TO</td>
</tr>
<tr>
<td></td>
<td>TORRENTSDOWNLOAD.ORG</td>
</tr>
<tr>
<td></td>
<td>FENOPY.EU</td>
</tr>
<tr>
<td></td>
<td>PRIMEWIRE.AG</td>
</tr>
<tr>
<td></td>
<td>SOLARMOVIE.EU</td>
</tr>
<tr>
<td></td>
<td>FREE-TV-VIDEO-ONLINE.ME</td>
</tr>
<tr>
<td></td>
<td>THEPIRATEBAY.ORG</td>
</tr>
<tr>
<td></td>
<td>YIFY-TORRENTS.COM</td>
</tr>
<tr>
<td></td>
<td>MOVIE4K.TO</td>
</tr>
<tr>
<td></td>
<td>WATCHFREEMOVIES.CH</td>
</tr>
<tr>
<td></td>
<td>VODLY.TO</td>
</tr>
<tr>
<td></td>
<td>THEPIRATEBAY.GY</td>
</tr>
</tbody>
</table>

### Proxy Sites with comScore Data Available (Page 2)

<table>
<thead>
<tr>
<th>Proxy Sites with comScore Data Available (Page 2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>COME.IN</td>
</tr>
<tr>
<td>PIRATEREVERSE.INFO</td>
</tr>
<tr>
<td>KATPROXY.COM</td>
</tr>
<tr>
<td>QUULUXINGBA.INFO</td>
</tr>
<tr>
<td>TORRENTCITY.COM</td>
</tr>
<tr>
<td>PIRATEPROXY.NET</td>
</tr>
<tr>
<td>KICKASS.PW</td>
</tr>
<tr>
<td>UNBLOCKED.CO</td>
</tr>
<tr>
<td>PIRATEPROXY.NET</td>
</tr>
<tr>
<td>KICKASS.PW</td>
</tr>
<tr>
<td>KICKASSUNBLOCK.INFO</td>
</tr>
<tr>
<td>PROXYDUCK.COM</td>
</tr>
<tr>
<td>TPBUNION.COM</td>
</tr>
<tr>
<td>BAYMIRROR.COM</td>
</tr>
<tr>
<td>UNLOCKTORRENT.COM</td>
</tr>
<tr>
<td>THELITEBAY.COM</td>
</tr>
<tr>
<td>OCCUPYUK.CO.UK</td>
</tr>
</tbody>
</table>

### Italy: Blocked Sites with Alexa Data Available (Page 6)

<table>
<thead>
<tr>
<th>Italy: Blocked Sites with Alexa Data Available (Page 6)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1337X.TO</td>
</tr>
<tr>
<td>BITSHARE.COM</td>
</tr>
<tr>
<td>TORRENTDOWNLOADS.ME</td>
</tr>
<tr>
<td>SHARE76.COM</td>
</tr>
<tr>
<td>TORRENTCRAZY.COM</td>
</tr>
<tr>
<td>FREAKSHARE.COM</td>
</tr>
<tr>
<td>TORRENT.CD</td>
</tr>
<tr>
<td>LASCENA.NET</td>
</tr>
<tr>
<td>THEPIRATEBAY</td>
</tr>
<tr>
<td>KICKASS.TO</td>
</tr>
<tr>
<td>NOWDOWNLOAD.CH</td>
</tr>
<tr>
<td>7TV.ORG</td>
</tr>
<tr>
<td>H33T.COM</td>
</tr>
<tr>
<td>MOVSHARE.NET</td>
</tr>
<tr>
<td>TORRENTHOUND.COM</td>
</tr>
<tr>
<td>TORRENTVIA.COM</td>
</tr>
<tr>
<td>CINEBLOG01.EU</td>
</tr>
<tr>
<td>CYBERLOCKER.CH</td>
</tr>
<tr>
<td>TORRENTROOM.COM</td>
</tr>
<tr>
<td>NOWVIDEO.CH</td>
</tr>
<tr>
<td>Uploaded.NET</td>
</tr>
<tr>
<td>UploadJET.NET</td>
</tr>
<tr>
<td>WATCHFREEMOVIES.CH</td>
</tr>
<tr>
<td>TORRENTZ.PRO</td>
</tr>
<tr>
<td>RAPIDGATOR.NET</td>
</tr>
<tr>
<td>NOWDOWNLOAD.CO</td>
</tr>
<tr>
<td>NOWVIDEO.CO</td>
</tr>
<tr>
<td>USEFILE.COM</td>
</tr>
<tr>
<td>ROJADIRECTA.ME</td>
</tr>
<tr>
<td>DDL-FANTASY.ORG</td>
</tr>
<tr>
<td>SUMOTORRENT.SX</td>
</tr>
<tr>
<td>QUEENSHARE.COM</td>
</tr>
<tr>
<td>LIMETorrents.COM</td>
</tr>
<tr>
<td>DDLHITS.COM</td>
</tr>
<tr>
<td>TORRENTDOWNLOAD.WS</td>
</tr>
<tr>
<td>FLASHSTREAM.IN</td>
</tr>
<tr>
<td>Videopremium.Me</td>
</tr>
<tr>
<td>Isohunt.TO</td>
</tr>
<tr>
<td>Extratorrent.cc</td>
</tr>
</tbody>
</table>

### Italy: Blocked Sites with comScore Data Available (Page 6)

<table>
<thead>
<tr>
<th>Italy: Blocked Sites with comScore Data Available (Page 6)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kickass.TO/Kat.ph</td>
</tr>
<tr>
<td>Extratorrent.cc</td>
</tr>
<tr>
<td>Videopremium.net</td>
</tr>
<tr>
<td>Vkontakte</td>
</tr>
<tr>
<td>Uploaded.net</td>
</tr>
<tr>
<td>Torrenthound.com</td>
</tr>
<tr>
<td>Cyberlocker.ch</td>
</tr>
<tr>
<td>Limetorrents.com</td>
</tr>
<tr>
<td>Bitshare.net</td>
</tr>
<tr>
<td>Freakshare.net</td>
</tr>
<tr>
<td>Rapidgator.net</td>
</tr>
<tr>
<td>Torrentdownloads.me</td>
</tr>
<tr>
<td>Nowvideo.co</td>
</tr>
<tr>
<td>1337X.org</td>
</tr>
<tr>
<td>Yourlifeupdated.it</td>
</tr>
<tr>
<td>Rojadirecta.me</td>
</tr>
<tr>
<td>Thepiratebay</td>
</tr>
<tr>
<td>Torrentcrazy.com</td>
</tr>
<tr>
<td>Clipshouse.com</td>
</tr>
<tr>
<td>Torrent.cd</td>
</tr>
<tr>
<td>Extratorrent.cc</td>
</tr>
<tr>
<td>Flashstream.in</td>
</tr>
<tr>
<td>Speedvid.tv</td>
</tr>
<tr>
<td>Torrentz.pro</td>
</tr>
<tr>
<td>H33t.com</td>
</tr>
<tr>
<td>Queenshare.com</td>
</tr>
<tr>
<td>Likeupload.net</td>
</tr>
<tr>
<td>Movshare.net</td>
</tr>
<tr>
<td>Sumotorrent.com</td>
</tr>
<tr>
<td>UploadJET.NET</td>
</tr>
<tr>
<td>Cineblog01.org</td>
</tr>
<tr>
<td>Torrentroom.com</td>
</tr>
</tbody>
</table>