ONLINE COPYRIGHT INFRINGEMENT – PUBLIC CONSULTATION

EXTENDED AUTHORISATION LIABILTY

1 September 2014

1. What could constitute 'reasonable steps' for ISPs to prevent or avoid copyright infringement?

We support the current approach taken by the courts, as summarised by High Court of Australia in *Roadshow Films Pty Ltd v iiNet Ltd* [2012] HCA 16, at paragraphs [75]–[78] (French CJ, Crennan and Kiefel JJ), [146] (Gummow and Hayne JJ). We respectfully agree with the Court's analysis of the current state of technology and the law. We do not consider there to be any obvious policy reason why the law should be altered so as to provide for a different definition of 'reasonable steps'.

As the Court explained, until an ISP receives evidence at least as strong as proof of infringement of copyright to the civil standard, there will not be a reasonable basis for an ISP to 'prevent or avoid copyright infringement', or indeed to take any steps at all. It is unclear whether this question refers to steps to be taken before or after the receipt of proof. Steps to be taken after proof of infringement by a subscriber would presumably be determined by the Court in any action against that subscriber. In this respect, we find the question posted by the consultation unhelpfully vague, and we urge the government to reconsider the underlying premise – ie, that ISPs should somehow be required to act in the absence of proof of infringement.

We emphasise at the outset that the discussion paper presents only part of the relevant background. The paper cites a 2011 PwC report to the effect that Australia generates £7 billion in copyright exports, but fails to cite the conclusion from the same report that Australia is clearly a net copyright importer, with a comparative £30.8 billion in imports. In 2013, Australia's exports of audiovisual and related material – frequently invoked in the rhetoric of copyright reform – were dwarfed by imports, and this is a consistent trend across the creative industries (see DFAT, 'Composition of Trade Australia: 2013' (June 2014) 50–52 <http://www.dfat.gov.au/publications/stats-pubs/cot-cy-2013.pdf>).

We are particularly surprised that the key policy assumption underlying the consultation paper – that requiring ISPs to take further steps to prevent infringement under threat of monetary liability would be effective – is not examined in any detail. It does not appear to be supported by empirical evidence and there is limited discussion of relevant experience in other jurisdictions such as the UK, where a narrow concept of authorisation liability has prevailed since long before the *iiNet* decision and where there is no suggestion that it needs to be expanded. We believe that the proposed reform would pose a far greater burden than asset to the Australian technology and telecommunications industries, and we would urge against the course proposed. That the consultation does not even permit consultation on the core premise but moves directly to detail is a very worrying indication that this proposal is not properly supported by an evidence base.

2. How should the costs of any 'reasonable steps' be shared between industry participants?

For the reasons we explained in answer to question 1, we do not consider that any further steps need to be taken by ISPs and so no issue of cost-sharing arises. However, to the extent that the government legislation is enacted to require more of ISPs, we think this question proceeds from a false premise.

As non-wrongdoers, the starting point is that an innocent party is not required to bear the costs of any enforcement action taken to cease facilitating wrongdoing. This is a cardinal principle of the common law. The government should carefully consider the decision of the House of Lords in *Norwich Pharmacal Co v Customs and Excise Commissioners* [1974] AC 133 (a case where the respondent was required to disclose evidence to assist the claimant rights-holder), where Lord Reid stated at 176 that any steps taken by the innocent defendant would be 'at the expense of the person seeking the disclosure' (ie, the rights-holder).

In the context of internet enforcement and copyright, the same principles apply: see *Totalise plc v The Motley Fool Ltd* [2002] 1 WLR 1233. In that case, Aldous LJ held that costs incurred by an innocent internet service (in that case a website operator) should be paid by the rights-holder, who would be free to recover them in due course from the ultimate wrongdoer. Only where an ISP is 'implicated in a crime or tort or seeks to obstruct justice being done' should it be required to bear its costs: at 1237 (Aldous LJ). This approach is essentially sound and we consider that the same approach would and should apply under Australian law.

As such, we would strongly urge the government to recognise that ISPs are not primary wrongdoers. Any steps they would be required to take would be to enforce private property rights of third parties. As such, the costs of that enforcement should be borne solely by rights-holders, unless the ISP is itself proved to be a primary wrongdoer.

3. Should the legislation provide further guidance on what would constitute 'reasonable steps'?

For the reasons we have explained in answer to question 1, we do not think it is appropriate to legislate to require ISPs to act in circumstances where they do not currently owe any duties to act.

Moreover, there is no need for any statutory notice-and-notice scheme. Rights-holders are already free to apply to a court for disclosure of subscribers' identities and can, if they wish, send notices to those subscribers alleging infringement. Courts, and not ISPs, remain the appropriate gatekeepers of that process, given its potential to interfere with the privacy rights of consumers as data subjects. That rights-holders find existing mechanisms insufficient suggests that they have not adequately employed existing mechanisms for disclosure of subscriber information, and are unwilling (perhaps for public relation reasons) to enforce their own rights against infringers. However, that embarrassment is not a valid reason for requiring ISPs to enforce those rights instead.

The international experience is telling. The US and NZ approaches – which, it must be noted, differ critically from the UK light-touch approach – are the exception and not the norm. Far from being the preferred or effective position, a comprehensive study published this year by Monash University

academic Rebecca Giblin, building on other work, concludes that there is little to no evidence that graduated response mechanisms are either successful or effective: see Rebecca Giblin, 'Evaluating Graduated Response' (2014) 37 *Columbia Journal of Law and the Arts* 147.

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?

N/A

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?

We are concerned that this question suggests a presumption that ISPs will be required to take action against consumers in the absence of a finding of copyright infringement against that subscriber, supported by adequate and admissible evidence. For the reasons we have indicated, any scheme or steps should be premised upon a finding of infringement by a court.

If this is not the government's preferred policy, that would render statutory guarantees for the quality of evidence, consumers' rights of appeal, and the burden of costs of such appeals, all the more important.

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

We consider that the approach taken in section 97A of the *Copyright, Designs and Patents Act 1988* (UK) is generally appropriate. Section 97A permits rights-holders to apply to a court for an order that a service provider cease the use of its services for copyright infringement, provided that the service provider has actual knowledge of the infringement. In practice, actual knowledge is easily satisfied by the sending of a pre-action notice (or indeed claim documents) to the ISP.

Section 97A applies more widely than ISPs. Because of the broad definition of service provider, it potentially includes website operators, search engines, and web hosts. We do not see any reason to restrict blocking orders to ISPs.

Section 97A has been interpreted broadly in a line of authorities of the High Court of England and Wales. We emphasise six key features of those authorities:

- First, the obligation is not absolute but is a requirement to take steps directed at disabling access to the website. The precise steps which must be taken are, by convention, delimited in detail in the order of the court and are tailored to the individual systems of the respondent.
- Second, blocking is discretionary and conditional upon a judicial finding of infringement by a third party, which is carried on the respondent's service.

- Third, blocking creates no monetary liability.
- Fourth, blocking must be a proportionate remedy in the circumstances, bearing in mind the cost of blocking, the impact on the respondent, the likely effectiveness of the order, the risk of blocking access to non-infringing content, and the available alternative remedies (such as notice-and-takedown against the primary publisher). The risk of overblocking, in particular, is a highly material factor, and orders have so far been made only against obvious safe-havens for infringing content.
- Fifth, blocking orders include a provision for updates. This is a judicial innovation and is properly a matter for the court to supervise. Updates are necessary for orders to have any hope at being even moderately effective, to reflect changes to the IP addresses and URLs of blocked websites. In the UK experience, updates to blocking orders are very frequent, with ISPs being asked to block hundreds of mirror websites for every blocking order that is made.
- Sixth, all of the major English ISPs already have well-established blocking systems in place, which they use to filter child abuse materials and in many cases to provide 'safe' internet services to parents. Those systems have received very substantial capital investment. To our knowledge, no orders have been made against ISPs that do not already possess capable blocking infrastructure. To do so would not be fair or proportionate.

The government should avoid an expansionist approach to delimiting any blocking remedy. A simple provision which permits the courts to engage in a wide proportionality analysis is desirable. Courts should, however, be required to consider certain mandatory factors, including effectiveness, cost, and negative consequences.

Additionally, ISPs as non-wrongdoers should not be required to pay for the costs of (i) appearing at and responding to an application for a blocking injunction; or (ii) implementing or implementing updates to the court's order. This follows from the principles outlined in answer to question 2.

7. Would the proposed definition adequately and appropriately expand the safe harbour scheme?

We encourage the adoption of safe harbours that are framed in technologically neutral terms. We can see no principled reason why safe harbour protection should be limited to "carriage service providers". The same justifications for safe harbour protection (impracticality, fairness, innovation, and chilling effects) apply equally to other providers of internet services. Service providers at the application, network, and physical layers of service provision should be included.

Although the European approach is a useful model, it poses several problems. Currently, the definition of "information society service provider" requires a service to ordinarily be provided for remuneration. This has led to confusion, particularly where service providers (although commercial) do not charge their users for access to the services, but instead rely upon advertising or other business models to generate revenue. Additionally, the framing of the European safe harbours creates difficulties where a service provider engages in activities which both fall within and outside the protected categories of activity (storage, caching and transmission); for example, a social network may store user-created content, but it may also process, rank and publish that content in ways which go beyond mere storage. The courts have found it difficult to apply the safe harbours to these kinds of mixed activities. We would encourage the government to be mindful of these problems when drafting

any amendments to the safe harbour provisions, and to avoid defining the preconditions unduly restrictively.

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

N/A

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

The discussion paper and proposal proceed on the assumption that ISPs may be held liable to compensate copyright owners for wrongdoing by their subscribers merely by providing those subscribers with Internet access. As we have explained above, we do not think this approach is justified. Rights-holders already have strong protections and enforcement mechanisms at their disposal, including the ability to obtain disclosure of the identity of primary infringers from any service provider. That ability does not require any statutory amendment – it already exists and is a well-established feature of the courts' equitable jurisdiction.

To the extent that the government is minded to create additional enforcement measures specifically addressed to the issue of internet infringement, we encourage the government to widen its thinking beyond the blunt instrument of monetary intermediary liability. For example, the government could, after appropriate consultation and evidence-gathering processes:

- provide for de-indexing orders against search engines;
- permit payment freezing orders against payment processors who fund or channel the proceeds of online infringement;
- facilitate the creation of codes of practice dealing with notice-and-takedown;
- strengthen the regime for border seizure of infringing goods;
- ensure that children and young adults are educated about copyright norms and encouraged to create, reuse and remix content; and
- most importantly, take steps to ensure that Australian consumers have a wide range of options to get affordable, timely and unfettered access to legitimate sources of the content they want.

Conversely, efforts by rights-holders to enlist ISPs as unpaid copyright enforcers are likely to be ineffective. Consumers will only become better at hiding their infringements. It will not address the fundamental cause of internet infringement, which is inadequate access to lawful sources of content and to continue facilitating the rapid growth in the uptake of source such as Netflix, Amazon Prime, HBO, Spotify, Google Play, and others – the vast bulk of which simply are not available to Australian consumers because of copyright licensing restrictions.

Our response to online copyright infringement should be measured and carefully considered. We repeat recent statements by the WIPO Director General, and Australia's most senior UN official, Francis Gurry: the solution to copyright infringement is to help consumers to take ownership of solutions to ensuring vibrant creative industries and adequate remuneration for creators. See, for

example: Francis Gurry, 'The Future of Copyright' (February 2011) <http://www.wipo.int/about-wipo/en/dgo/speeches/dg_blueskyconf_11.html>.

Resources expended on educational notices and on ISP enforcement regimes should be directed instead into providing lawful access that is readily accessible, fairly priced, and portable across devices.

Online infringement will only be reduced by responses that show leadership and that recognise the sources of discontent. As a net importer of IP, Australia has a real opportunity to be a leader for forward-looking measures. By way of example, we think that the following measures are more likely to combat internet infringement than would the government's proposal on ISP liability:

- First, reasonable prices.
- Second, access to content in a timely manner (that is, contemporaneously with international broadcasts and release dates).
- Third, guarantees that consumers will not have their rights shackled by DRM technology that controls how they can use and enjoy content that has been lawfully purchased.
- Fourth, protection of consumers' interests in relation to digital content, including the ability to freely re-download files that have been accidentally deleted or lost, or to transfer between platforms.
- Fifth, the option both to stream media on a subscription basis and to purchase more durable physical copies.
- Sixth, making proper provision for access for people who can't afford to pay (this might require us to look again into the concept of funding and equipping proper public libraries for all forms of media).
- Seventh, a much closer look at the differences between different industries. The traditional publishing sector is not nearly as vocal as the music and film industry in relation to infringement. The reasons, causes, and implications of this should be fully explored.

10. What regulatory impacts will the proposals have on you or your organisation?

N/A

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

Expanded authorisation liability could carry a host of unintended consequences. First, if the definition of 'reasonable steps' applies generally, there is a significant risk that that will expose small businesses to greater risk of liability to conduct by their customers, users and suppliers. Second, it may stifle Australia's burgeoning start-up economy by preventing 'disruptive' start-ups from being able to grow into the next Facebook, Google or eBay (all of whom relied upon safe harbours and narrower authorisation liability in order to rise to positions of incumbency). That stifling may occur directly, though industry lawsuits, or indirectly, through a perception of liability risk (rightly or wrongly) which leads those businesses not to receive capital investment at their early stages. Third, other service providers that have more direct control over data (for example, those that store content in some material form, rather than merely transmitting it) may face unintended liability.

Fourth, other creators of content may find their lawful material pre-emptively removed by a service provider out of fear of liability. We are particularly concerned by the potential that wider monetary liability would lead to 'chilling effects' of this kind. For this reason, whatever the government's chosen policy, it should ensure that strong deterrents are in place to discourage unjustified threats of infringement such as wrongful take-down notices. It may also wish to legislate for mandatory 'put-back' procedures that apply upon a counter-notification being made by a third party, similar to those that have been available in the United States since the enactment of the *Digital Millennium Copyright Act* in 2000.

We thank the government for the opportunity to respond to the consultation and hope that our comments are helpful.

Yours sincerely

Dr Jaani Riordan
Barrister, Lincoln's Inn, London

Julia Powles
PhD Student, Faculty of Law, University of Cambridge