THE LEGAL PERILS OF BEING AN INTERNET SERVICE PROVIDER

David Lindsay
Guest Editor

This edition of the TJA focuses on a range of stimulating and difficult legal issues that face intermediaries, especially ISPs, in performing their vital functions of providing access to communications content.

Over the past 15 or more years, we have become familiar with the radically destabilising impact of the Internet on established economic, social, legal and political structures. In relation to the delivery of information and entertainment content, the Internet has provided unprecedented and welcome access to all manner of content but, at the same time, decentralised Internet-based applications, especially P2P networks, have been engines for large-scale copyright infringement.

The highly politicised struggles over copyright – commonly known as the 'copyright wars' – are but one instance of the disruptive influence of the Internet on existing legal structures. An important aspect of these struggles arises from what is inelegantly referred to as 'disintermediation' – which, in this context, means the lessening influence of the traditional gatekeepers or intermediaries responsible for communications content, including publishers, the press and broadcasters. In place of the traditional intermediaries, which perform a role in the creation as well as the distribution of content, and therefore have an uncontested degree of legal responsibility for that content, we have seen the emergence of 'new' intermediaries, in the form of ISPs, search engines and social network service providers.

These new intermediaries have business models that rely essentially upon commercialising access to content. While they may well produce some content, in general they do not have to bear the costs of content creation. Nevertheless, given the costs and futility of bringing legal actions against individual end-users, the extent to which these intermediaries may be liable for the actions of their end-users has become one of the great legal issues of the Internet era. This issue inevitably raises complex policy issues relating to the proper role of access providers in 'policing' the behaviour of their users, the degree to which access/carriage providers should become involved in content issues, and the costs and benefits of enforcing offline legal rights in the online environment.

THE 'GRADUATED RESPONSE'

From the mainstream emergence of the Internet in the mid-1990s, carriers and ISPs have been concerned about their potential liability for copyright infringements committed by their customers. As a result, telecommunications companies first became involved with international copyright policy-making in the negotiations leading to the adoption of the two 'Internet treaties' – the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT) – in 1996. The concerns of carriers and ISPs that the potential for liability might adversely impact their role as access providers led to an Agreed Statement being added to the WCT, which provided that 'the mere provision of physical facilities for enabling or making a communication' would not, in itself, amount to an infringement of the exclusive right to communicate copyright material. Subsequently, in jurisdictions such as the United States and Australia, a degree of legal protection for some intermediaries was

established in the form of what is known as a 'safe harbour' regime, pursuant to which intermediary liability is limited provided an intermediary, such as an ISP, takes certain steps, such as adopting and implementing a policy for dealing with users who repeatedly infringe copyright.

Meanwhile, from the emergence of Napster in 1999, we have seen the evolution of generations of popular P2P file-sharing applications – culminating with the BitTorrent protocol – that provide efficient, decentralised mechanisms for end-users to distribute content, and which are difficult to police and control. The prevalence of end-user copyright infringements, and the failure of other means of controlling digital content, such as technological protection measures (TPMs), led the content industries, in the mid-2000s, to advocate a policy known as 'graduated response'. The 'graduated response' strategy, which is also known as 'three strikes', aims to curb online copyright infringements by enlisting the help of ISPs in issuing warnings to repeat infringers, and ultimately suspending or terminating the accounts of recalcitrant end-users.

Versions of 'graduated response' have been introduced in a number of countries. In Australia, the complex copyright regime governing the liability of ISPs for end-user infringements was premised on the development of an industry code of practice, which would deal with the detail of how ISPs should respond to infringement notices issued by copyright owners. While representatives of copyright owners and the Internet Industry Association (IIA) entered into negotiations aimed at developing a code, nothing eventuated. Given this impasse, the Australian Federation Against Copyright Theft (AFACT), which is effectively the Australian investigation and education arm of the copyright owners, sent details of large-scale infringements committed by customers of iiNet, and 'required' that the ISP take appropriate action.

Following iiNet's persistent refusal to take the action sought by AFACT, the copyright owners initiated an action claiming that iiNet's inaction, in the face of the information provided by AFACT, rendered it liable for the infringements of its end-users. The first article in this edition, by Lindsay, analyses the landmark Australian High Court decision in *Roadshow Films v iiNet*. As the article explains, the clear result of the first decision on this issue, in any part of the world, by the highest court in a jurisdiction is that an ISP that does no more than provide Internet access will not be liable for end-user infringements, unless it does something unlikely, such as actively promoting unlawful downloading. As the article further explains, however, the judgments in the High Court have effectively changed the Australian law on secondary liability for copyright infringements, opening up a host of new legal questions.

The High Court decision in *iiNet* means that the implementation of a graduated response strategy in Australia depends, in the first instance, upon negotiations on a proposed code between the copyright owners and ISPs, with the Commonwealth Attorney-General's Department brokering negotiations between AFACT and the Communications Alliance. A sticking point in the negotiations has been who should bear liability for the costs of implementing a graduated response regime. If the parties are unable to reach agreement, the future of graduated response in Australia will depend upon the willingness of the Parliament to introduce a legislative regime. At present, there is no indication that this seems likely. While the government has issued an important reference on copyright and the digital economy to the Australian Law Reform Commission (ALRC), the reference is confined to copyright exceptions, with the ALRC being specifically instructed not to duplicate work being undertaken on unauthorised distribution of copyright materials using P2P networks.[1]

In contrast to the position in Australia, some jurisdictions – New Zealand, France, the United Kingdom, Taiwan and South Korea – have introduced laws implementing forms of graduated response, each of which has proven controversial. The second article in this edition, by Rebecca Giblin from Monash Law School, examines the New Zealand regime, which was implemented by the *Copyright (Infringing File Sharing) Amendment Act 2011*. After an analysis of the regime, Giblin concludes that it is unlikely to achieve the objective of deterring unauthorised file-sharing, given the costs of implementing the regime, an unintentional

loophole in the regime and the absence of any measures to encourage the creative industries to adapt to delivery of content via the Internet. More fundamentally, Giblin argues that graduated response strategies are flawed in that suspension or termination of Internet access is a disproportionate response which may infringe user rights and that they do not deal with the true source of the problem of unlawful downloading, which she identifies as the failure of copyright industries to provide timely and reasonably priced content.

In the following article David Brennan, from Melbourne Law School, compares and contrasts the voluntary graduated response regime, entered into between copyright owners and large ISPs in the United States, with the French legislative regime, which is known as *HADOPI*. After explaining that, under US law (as in Australia post-*iiNet*), it is unlikely that ISPs that merely provide access will be liable for end-user infringements, Brennan suggests that the US 'five-strikes' regime may have resulted from a 'behind-the-scenes' role played by the Obama administration, as well as the threat of possible legislative intervention. In contrast to the Giblin article, Brennan refers to a recent report from US academics which concludes that the introduction of *HADOPI* resulted in a significant increase in lawful downloads from iTunes in France.[2] From the American and French experiences, Brennan draws the lesson that the threat of introducing a *HADOPI*-style law may be essential for a US-style voluntary regime to be negotiated in Australia. Whatever the case, it seems that, in regimes that have introduced graduated response regimes (whether private or public), we will face ongoing debates about the effects of those regimes on user behaviour, including debates about the methodologies employed in academic and industry studies.

INDUSTRY AND USER RESPONSES

The fourth article in this edition, by Neil Gane, the Managing Director of AFACT, explains how, from the point of view of copyright owners, graduated response is necessarily part of a broader strategy for dealing with the problem of P2P file-sharing. According to Gane, there is no silver bullet, but an effective strategy must involve regulation, partnerships between the content and telecommunications industries, and ongoing user education. Importantly, Gane points out that there is a growing commonality of interests between the telecommunications and content industries, as carriers and ISPs are increasingly concerned with monetising content. Nevertheless, drawing from comments made by Charleton J in the Irish High Court, he concludes that the decision in *iiNet* has revealed that the current Australian law is inadequate to deal with P2P file-sharing, and calls for legislative intervention.

In the following article, Holly Raiche, from the Internet Society, argues that the user-perspective has been missing from debates about the appropriate response to P2P file-sharing. While agreeing with Gane that education is an essential part of any solution to the problem, Raiche proposes elements of a regulatory response that would effectively incorporate user rights and interests. Apart from the importance of user input into any code development process, she maintains that, from a user perspective, any code must: not automatically equate the account holder with alleged infringers; respect the privacy of account holders; incorporate an effective appeals mechanism; and include account termination only as a last resort. Over and above the details of a proposed code, Raiche points out that the focus on unlawful downloading should not blind us to the integral role now played by the Internet in peoples' lives, suggesting that any responses to the problem must be kept in proportion.

ADDITIONAL ONLINE COPYRIGHT DILEMMAS

Copyright controversies involving carriers, ISPs and other intermediaries are not confined to their potential role in relation to P2P file-sharing. Two further articles in this edition examine two recent important legal controversies.

Users are increasingly taking advantage of cloud computing to access material when and where (and on which device) they want it. The mismatch between cloud computing and copyright law in Australia has been highlighted by a service provided by Optus, known as TV

Now, which sought to take advantage of an exception to copyright that allows viewers to make copies of broadcasts for later viewing for their own private use. The Optus service enabled users to record television programs on an Optus server, which allowed users to access the recorded programs on their mobile and Internet devices. In practical terms, a user could access a live broadcast of a football game from a mobile or Internet device with only a two minute delay. This obviously alarmed the rights owners in football broadcasts – Telstra, the AFL and the NRL – as, if Optus could take advantage of the private use exception it could effectively provide a service involving near-live streaming without paying the rights owners.

Warwick Rothnie, from the Victorian bar, clearly and thoroughly explains the complex legal issues in the Optus TV Now litigation, focusing on the decision of the Full Federal Court, which held that Optus was not entitled to the exception. As Rothnie points out, the decision gives rise to a number of significant legal issues for which the Copyright Act provides no clear answers. At the time of writing, an application for leave to appeal to the High Court has been made, but the outcome of the application is unknown. Regardless or whether or not the High Court agrees to hear the appeal, the scope of the private use exception relied upon by Optus will be dealt with in the ALRC copyright exceptions review, mentioned above.

If one thing is certain, the copyright wars are far from static, with the strategies of owners and infringers continually evolving against a background of shifting technologies and markets. Earlier this year, controversial US legislative proposals for enlisting a range of new intermediaries – domain name servers, credit card providers and online advertising service providers – in online copyright enforcement, were withdrawn from Congress. The article by Kim Weatherall, from the University of Sydney, explains and analyses the most important of the US legislative proposals, known as *SOPA*. As Weatherall explains, if implemented, *SOPA* would have effectively enabled a 'multi-system denial of service' attack on 'rogue' web-sites, such as The Pirate Bay, by preventing the DNS from resolving to the site, requiring search engines to eliminate links to the site, requiring US credit card companies to refuse payments to site operators, and prohibiting US companies from advertising on such sites. While, following considerable online outrage, *SOPA* was withdrawn, Weatherall focuses on the fundamental implications of the proposed regime for more general arguments for imposing liability on intermediaries. On this, Weatherall concludes that the argument that liability should be attached to intermediaries on the basis that this is an efficient approach to enforcement – known as the 'least cost avoider' argument – is flawed, as it ignores other important considerations, including whether the overall costs of imposing liability outweigh any benefits, and longer term negative consequences that might follow from imposing liability. In addition to the important points made by Weatherall, the *SOPA* saga suggests that there may be real political limitations on the extent to which liability can be attached to access intermediaries, especially as the increased lobbying power of access providers, such as Google and Facebook, is effectively brought to bear.

OTHER ISSUES FOR INTERMEDIARIES

Controversies concerning the role, and potential legal responsibilities, of intermediaries are by no means confined to the copyright context. Two articles in this edition examine the role of Internet intermediaries in a broader context.

The first of these, by Melissa de Zwart from the University of Adelaide, focuses on one of the most prominent examples of disintermediation, WikiLeaks. As de Zwart explains, WikiLeaks is essentially an intermediary that was intended to be a mere conduit for the publication of material sourced from whistle-blowers, but which, because of circumstances, evolved so that Assange, the public face of WikiLeaks, assumed a more 'hands-on' role. Nevertheless, the relatively unmoderated nature of publication via WikiLeaks serves not only to distinguish it from traditional media, but also to explain much of the concern of governments, especially the US government, with the WikiLeaks model. The second part of the de Zwart article provides an interesting companion-piece to Weatherall's analysis of the *SOPA* saga, in that it explains and analyses the use of financial intermediaries, including PayPal, Mastercard and VISA, to deny processing of payments to WikiLeaks. According to de Zwart, given that the financial

intermediaries denied payments on the basis of an allegation that WikiLeaks had breached their terms of service, this illustrates the troubling extent to which online regulation and enforcement has been privatised. In effect, the activities of WikiLeaks, which are located largely outside the US (and which may not be illegal even in the US), could be effectively denied resources without any proper legal process.

In the second of these articles, Alana Maurushat, from the UNSW Cyberspace Law and Policy Centre, examines the role of ISPs in combating botnets. The article summarises and explains the four main methods of tackling botnets, pointing out that ISPs play a role in all but one of these methods. As Maurushat points out, ISPs are generally not regarded as being responsible for the security of their customer's computers, or for monitoring content. However, recent Australian proposals detailed in the article, including the e-Security Code, incorporate a greater role for ISPs in dealing with end-user security. Based upon the uncontested need to ensure network protection and security, Maurushat argues that effective botnet remediation programs can only be implemented with active intervention by ISPs. While necessary, such intervention should be restricted to protect users and their privacy by, for example, being limited to small and medium packet inspection and passive monitoring. Importantly, the article argues that ISPs cannot be expected to adopt a greater role in combating botnets without the protection of legal limitations on liability, which go beyond that conferred by the 2010 amendments to the *Telecommunications (Interception and Access) Act*. Read together with the other articles in this edition, the article illustrates not only the complexity of the issues involved with the legal liability of intermediaries, but the importance of avoiding high level generalisations, and taking into account the particular context, in developing laws and policies relating to the vital role of intermediaries in the online environment.

As guest editor for this edition of the TJA, I would like to thank each of the authors for the care, diligence and expertise with which they have addressed the particular issues dealt with in their contributions. Overall, the collection represents an important snapshot of many of the important 'live issues' in this area as of mid-2012.

ENDNOTES

1. Terms of Reference, *Copyright and the Digital Economy*, 29 June 2012, at http://www.alrc.gov.au/inquiries/copyright/terms-reference.

2. Brett Danaher, Michael D. Smith, Rahul Telang and Siwen Chen, 'The Effect of Graduated Response Anti-Piracy Laws on Music Sales: Evidence from an Event Study in France', Version as at March 2012, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1989240 (visited 20 July 2012).

Cite this article as: Lindsay, David. 2012. 'The legal perils of being an Internet Service Provider'. *Telecommunications Journal of Australia* 62 (4): 51.1-51.5. Available from: http://tja.org.au.