New Internet law confirmed after Federal Court cracks down on hyperlinker and ISP

Alan Arnott, Deacons

Alan Arnot is a lawyer and computer scientist in Sydney practising in Deacons' Technology, Media & Telecommunications Group.

Introduction

This article discusses the important recent Federal Court judgment handed down in *Universal Music Australia Pty Ltd v Cooper* on 14 July 2005. In this case, Justice Tamberlin ruled that the webmaster[1] and Internet Service Provider (**ISP**) that operated and hosted the *MP3s4free* website were liable for authorising Internet users to infringe copyright in pirated sound recordings in MP3 format accessible via hyperlinks on the website. The case was a first in several respects. It was the first time the new ISP safe harbours introduced by the Australia-United States Free Trade Agreement (**AUSFTA**) have been judicially considered. It was also the first time that an Australian court has ruled on the legality of websites that hyperlink to pirated content. In fact, it was the first time that the legal risks that flow from hyperlinking, the most prevalent technology used for navigation on the World Wide Web, have been considered by an Australian court at all. The case was delivered in the wake of the landmark decision handed down in the United States in *MGM v Grokster* only 17 days earlier that knocked two major players in the lucrative online peer-to-peer (**P2P**) file sharing industry off their feet and shook copy-device manufacturers around the world. The case follows in the footsteps of the US decision as a warning bell to Australian ISPs, webmasters, IT providers and their employees that there is not just a real danger in encouraging end users to use provided services for illegal means; IT providers and employees who exhibit a degree of indifference or fail to take steps to prevent or avoid infringement are also at risk.

Background

The proceedings were brought by a staggering thirty-one applicants, including music industry behemoths of the likes of Universal Music Australia, Warner Music Australia and Mushroom Records.

The 1st respondent, Stephen Cooper, owned and operated a popular website accessible via the URL *www.mp3s4free.net*. Cooper's website, known in the IT industry as a *warez* site, contained a highly structured database of categorised hyperlinks to popular sound recordings including those on the Australian Top 40, Billboard 50 and European charts. Internet users who clicked on the hyperlinks were given free reign to download (i.e. *copy*) the hyperlinked MP3s.

Cooper did not charge Internet users for access to his website. Instead, he employed a popular e-commerce business model known as *pay-per-click* advertising where advertisers pay according to the number of hits (i.e. *visits*) recorded on the relevant website. Cooper's website was so successful that the access log file seized when Cooper's ISP was raided on the execution of *Anton Piller* orders found that the website received 214,000 unique hits in a space of only 12 days.

The technical details of the website in this case are especially important: Cooper did not update the hyperlinks on his website personally. Instead, he provided a Common Gateway Interface (CGI), a web-based mechanism that allowed third parties to supply and edit the hyperlinks themselves. In addition, he did not store the MP3 files on his website. They were stored by third parties at arbitrary Internet locations.

Mindful of the possible consequences of his legally precarious entrepreneurialism, Cooper published terms and conditions on his website with explicit disclaimers he thought would absolve him of any liability he incurred through the site. How wrong was he.

There were four other respondents. The 2nd and 3rd respondents, E-Talk Communications Pty Limited and Com-Cen Pty Limited, conducted an ISP business which hosted the *mp3s4free.net* website for free in consideration for Cooper displaying the Com-Cen logo on his homepage.

The 4th respondent, Liam Francis Bal, was the principal and director of the ISP. The 5th respondent, Chris Takoushis, was an employee who worked at the ISP and was Cooper's primary contact at all relevant times.

Decision

The approach of the Court in dealing with each claim should be analysed with a fine toothcomb by all IT providers and in particular, webmasters, programmers and ISPs, to gauge their own liability. However, it is beyond the scope of this article to examine each aspect of the decision. The most noteworthy are set out below.

The first claims dealt with by the Court were those brought against Cooper for breach of the *Copyright Act* 1968 (Cth), which generally provides copyright owners with the exclusive right to exploit the copyright in their works. The Court found that:

- Cooper was liable under s101. That section sets out the regime for determining whether a person has infringed, or authorised another person to infringe, the rights of a copyright holder by doing acts that only the copyright owner is entitled to do. Cooper was found liable because he *"permitted or approved, and thereby authorized, the copyright infringement by Internet users who access his website..."*[2]

- The Court held that the disclaimers on the website did not amount to reasonable steps to prevent or avoid copyright infringement and that in contravention of the law laid down in *University of New South Wales v Moorhouse* by Gibbs CJ at 13, Cooper *"abstained from action which under the circumstances then existing it would have been reasonable to take, or...exhibited a degree of indifference from which permission ought to be inferred".*[3]
- Cooper could not rely on the s112 defence that *"has the effect of expressly limiting the authorisation liability of persons who provide facilities for the making of, or facilitating the making of, communications"*[4] because he *"offered encouragement to users to download offending material, as evidenced by the numerous references to downloading material on the website, and has specifically structured and arranged the website so as to facilitate this downloading".*[5]

In relation to the 2nd to 5th respondents, the Court found that:

- Although Bal and Takoushis argued that they did not even visit Cooper's website, the Court did not accept that they were unaware of its nature.
- Like Cooper, they breached s101 by authorising infringement since they *"were responsible for hosting the website and providing the necessary connection to the Internet and therefore had the power to prevent the doing of the infringing acts. They could have taken the step of taking down the website. Instead, they took no steps to prevent the acts of infringement."*[6]
- They could not rely on the protection offered by s112E that has the effect of limiting the authorisation liability of ISPs *"merely"* where another person uses the facilities to infringe copyright as they did more than *"merely"* provide facilities for the making of communications. For example, *"the reciprocal consideration passing between them, namely, the free hosting in return for the display of the Com-Cen logo on the website, is an additional matter which takes the situation beyond the protection afforded by s112E."*[7]
- They could not rely on the safe harbours introduced by the *US Free Trade Agreement Implementation Act* 2004 (Cth) which exclude liability for damages for copyright infringement. Firstly, the amendments do not operate retrospectively, that is, in relation to infringement that occurred prior to 1 January 2005. Secondly, the defence requires that an ISP must demonstrate that it has adopted a policy to sanction copyright infringers. Bal and Takoushis had emphasised that they were *"indifferent to the use that Cooper made of the facilities provided by E-Talk/Com-Cen. This falls far short of demonstrating that they had adopted a policy to sanction infringers."*[8]

Implications

The recent cases have tackled infringement whether ensuing from P2P, hyperlinking or offline technologies. These cases confirm the importance of maintaining robust risk management policies that deal with authorisation liability across all technologies, and highlight the Government's technology-neutral stance against copyright infringement that was adopted as part of the Digital Agenda amendments incorporated into the *Copyright Act* in 2000.

Readers of these cases will recognise that the Courts have placed a more onerous regime on technology providers that requires a closer monitoring of the services being provided. In determining authorisation liability, Australian Courts will generally look at:[9]

(a) the extent (if any) of the person's power to prevent the doing of the act concerned;

(b) the nature of any relationship existing between the person and the person who did the act concerned; and

(c) whether the person took any other reasonable steps to prevent or avoid the doing of the act, including whether the person complied with any relevant industry codes of practice.

Providers may prefer to rely on the protections afforded by the AUSFTA safe harbours. They require the adoption of policies to sanction infringing end users, termination of the accounts of repeat infringers and compliance with relevant industry codes.[10]

The judgment that has been handed down in the *MP3s4free* case is a precursor to the decisions yet to be delivered in the Australian *Kazaa* and *Metro on George* cases that will deal with P2P provider and nightclub owner authorisation liability respectively. Those decisions will serve to provide further clarification on the law of authorisation liability for the Australian IT and media industries.

---

1 Webmasters typically design and/or maintain websites. In this case, the webmaster was also the owner of the website.

2 At 84.

3 At 87.

4 At 98.

5 At 99.

6 At 121.

7 At 131.

8 At 107.

9 s 101(1A).

10 s116AH of the *US Free Trade Agreement Implementation Act* 2004 (Cth).