Volume 11 Number 3
Print Post Approved 24437100049

Contents

Information contained in this newsletter is current as at June 2008

Revisiting meta tagging with intent: sharp practice or smart practice?

Catherine Logan HUNT & HUNT

Your client is a big corporate with a big reputation in the real world — its brand is very valuable. It doesn't need to rely on website optimisation to attract new customers.

Its trading name is a registered trade mark and is frequently used by its competitors when meta tagging their own websites. The effect of this has been (though it is becoming less significant as search engine technology becomes more sophisticated), that when somebody searches your client's trading name, search engines such as Google will include competitors' sites in the search results, with the possibility that searchers (among them potential new customers) will be effectively diverted to the competitors' offerings.

More importantly, your client's trade mark is being used as a keyword trigger in the competitors' paid advertising, such as Google AdWords, with the effect that the competitors' sites come up in the 'sponsored links' in the search results.

While not wanting or needing to engage in a similar practice, your client is put out by this. In fact, that is an understatement. In any real-world scenario where a third party (particularly a competitor) wants to ramp up their business by using your client's valuable intellectual property, such as its registered trading name, it would be doing it only with the consent of your client, and paying handsome licence fees or royalties for the privilege.

Your client's reputation, after all, has been built up over years of hard work, and the idea that just because it is the World Wide Web someone else can piggyback on it is galling, to say the least. Surely, your client says, this conduct is an infringement of our trade mark or some other legal requirement and can be stopped? After all, this practice has been around now for nearly as long as the internet, well over a decade — surely I'm not the first one to complain? This article attempts to answer that question in light of current cases.

What are meta tags and keyword triggers?

Meta tags are HTML source code behind the user interface on a web page. They contain various pieces of information about the page. These may be keywords, but can also include descriptions of the page and ratings.

Meta tags are invisible, unless you deliberately choose to view them by selecting 'source' or 'page source' from the view menu on a web page. But the meta tag is what search engines have used in the past to select particular web pages in response to a user's search request. Use of meta tags, and keyword triggers in paid advertising, will determine whether that web page will be brought up in the list of results for the search of the tagged word or phrase.

Not use 'as a trade mark'

Meta tags are therefore not, in the trade mark sense, being used use as a badge of origin of the goods. In other words there is no 'use as a trade mark' such as would found an action for infringement of a registered trade mark under the *Trade Marks Act 1995* (Cth) (assuming your client's trade name is a registered trade mark, of course).

The current position under UK trade mark legislation would seem to be the same in that, despite some early cases in which the practice was viewed as trade mark infringement[1], it has been suggested by the full Court of Appeal in *Reed*[2] as possibly not being a use 'in the course of trade' as the legislation requires because of the invisibility of the tags themselves, though the court reserved its opinion on this point.

In that case it was necessary for the claimant, if it was to succeed, to also show user confusion had been caused, because the phrase used as a meta tag was not identical to the claimant's tag (and was in fact a trading name of the respondent). The trial judge's finding of infringement was overturned because 'causing a site to appear in a search result, without more, does not suggest any connection with anyone else',[3] and will not confuse users because they expect the results of their web searches to be littered with rubbish results. The court further stressed that the intent of the tagger is irrelevant in the context of trade mark infringement.

Passing off?

The momentary confusion and uncertainty in the mind of the consumer that this practice in its simplest form creates, is traditionally not sufficient to found a claim in what is, after all, a tort. For a claim in passing off to have any chance of success, claimants are required to prove that users have been deceived into thinking that the two competitors are connected, or at least that the alleged wrongdoer deliberately set out to mislead, deceive or cause confusion in the mind of the user, even if confusion was dispelled when the user eventually realised that he or she has accessed the competitor's website instead.

In *Reed*,[4] the first instance finding of passing off was overturned on appeal because 'No-one is likely to be misled — there is no misrepresentation'.[5] It was noted in the judgment that the respondent's website (which had a completely different name to the complainant's), came up below the complainant's in the search results.

Trade practices to the rescue?

If a user is directed to a competitor's web page by the use of your client's trade mark, is this misleading and deceptive conduct such as would found an action under the *Trade Practices Act 1974* (Cth) (the TPA)?

The answer to this will almost certainly depend on the particular facts and circumstances of your client's case.

If, for example, the meta tag used is a trading name, and all that is achieved by the use of the meta tag is that a competitor's website comes up in a list of search results, including your client's site, then it is hard to say that the user has been misled, especially if the competitor's website is clearly marked as such.

If, on the other hand, the search results are not clear in that regard, but the competitor's listing in the results somehow suggests a connection between the competitor's listing and your client or your client's website, this is akin to the competitor hanging your client's shop front sign out the front of its online business, and as such is not only sharp practice, but amounts to engaging in misleading and deceptive conduct and making false or misleading representations in contravention of ss 52 and 53 of the TPA.

The deception has to be fairly convincing as it has often been held that a reasonable web user will not normally treat the results of a web search with any particular reliability.[6]

Using a product or service name as a meta tag, another common practice, is also likely to be similarly unlawful if the product or service is not actually available through the competitor's website or business, but the results suggest that it is.

The fact that the user often quickly overcomes their confusion and does not end up dealing with the competitor is not a defence for the competitor in these circumstances.[7] It is well established that transitory effects do not affect the fact that the conduct is misleading and will only be relevant in considering whether or not an injunction should be granted.[8]

It has been suggested that the requirement for the conduct to be 'in trade or commerce' may defeat such claims, but as the use of meta tags is a marketing activity it seems to have the requisite trading or commercial character to fulfil this requirement. To suggest the use of meta tags is not conduct in trade or commerce is to fail to recognise its importance to the overall marketing strategy of the businesses that use it.

It may be a form of unpaid advertising, but is of no less significance than spam, or other direct marketing practices, and in some businesses is much more so,

To suggest the use of meta tags is not conduct in trade or commerce is to fail to recognise its importance to the overall marketing strategy of the businesses that use it.

particularly in start-up situations where there is no access to an existing mailing list. As for it being 'unpaid', this certainly does not mean there are no resources allocated to it. On the contrary, search engine optimisation, including meta tagging, is often outsourced to specialists and the appropriate fees paid. In some businesses it may be undertaken in-house utilising dedicated staff.

The major issue for complainants to overcome in making out a misleading and deceptive conduct claim will be the substantive one of whether in fact the overall effect of the conduct is, or is likely to, mislead or deceive.

It is submitted that in this way the TPA will allow complainants to address the truly unlawful instances of this conduct (those that are likely to confuse consumers), while not outlawing those that result in the user simply being provided with more information about the market allowing comparisons to be more easily made between competitors.

Australian case study

Legal precedent in Australia is thin on the ground, but it is interesting to note that in one case, *Kailash Center for Personal Development Inc v Yoga Magik Pty Ltd*, [9] where the owners of a website (Yoga Magik Pty Ltd and Meghan Stevens aka Gayenand) were found to have engaged in misleading and deceptive conduct in associating a third party (Jonn Mumford aka Swami Anandakapila Saraswati) with their website and the material on it.

In its final claim at the hearing the claimant did not specifically seek, and accordingly the relief ordered did not include, changing the meta tags on the website so that they no longer contained Mumford's name. This was because by the time of the hearing this had already been done. The respondent had, in the period leading up to the hearing, agreed to 'remove "offending" meta tags' as part of an attempt at 'accommodating the demands of the applicants'.[10]

It is interesting that the meta tags aspect of the claim (which was but one of many) was recognised by the respondent as being something that she was prepared to address before the hearing.

Do those who engage in this practice recognise it as a short-term game, one which they will readily forfeit at the first sign of trouble?

The author's personal experience bears this out. I was asked to demand on behalf of a client that a website owner change their meta tagging, and found they had done so before I had the chance to send a letter of demand. This was done apparently on the strength of my client's earlier email to the website owner.

Contrast the US position

The US has been a fertile source of case law on this subject since the late 90s owing to the *Lanham (Trade mark) Act (15 USC)* (the Lanham Act) and what has become known as its statutory unfair competition provisions. The doctrine of initial interest confusion developed in these cases has allowed claimants to make out a prima facie case even where confusion was transitory only, though in some cases defendants have been successful in claiming fair use in their defence, where the claim was based on the trade mark infringement section of the Lanham Act.[11]

Section 1125 of the Lanham Act, on the other hand, while it is part of a trade marks statute, to Australian eyes blends elements of ss 52 and 53 of our *Trade Practices Act* in a provision that prohibits the use of 'any word, term, name, symbol or device, or any combination thereof' which is likely to cause confusion as to the origin of the goods or services, or misrepresent the 'nature, characteristics, qualities or geographic origin' of the goods or services.

This section has, not surprisingly, provided a cause of action for complainants in cases where confusion is likely to arise through a party's conduct even though the elements of trade mark infringement have not been made out.

That part of the section that contains the wording giving rise to the statutory right of civil action does not even mention trade marks. This section has been described as providing a statutory right to claim unfair competition, but it is really a much narrower remedy, relying on either confusion or misrepresentation in commerce in connection with goods and services. In other words, it is a remedy that is more akin to ss 52 and 53 of the Australian TPA than anything in the Australian trade mark law, but in fact much more prescriptive than TPA remedies.

It does appear that the US law has provided stronger protection for owners of trade names in this area over the years, but it is submitted that the existence of the TPA remedies obviates the need for Australian trade mark reform along the lines of the US trade mark legislation, particularly given the declining significance of meta tags in recent years to the way in which search engines operate.

Comparative advertising

There is no doubt that in the process of legitimate comparative advertising the addition of meta tags to a web page referring to the competitor who is being compared to a web page is unassailable under our trade marks law[12] but if the content of the comparison is deleted from the web page, it is surely illegitimate to retain the meta tags.

If the remedy is not to be found under trade marks law, it is likely that the failure to remove the tags will qualify as unlawful misleading and deceptive conduct, depending of course on the overall effect of the conduct, as discussed above.

Meta data

As usual, just when the law finally starts to catch up, the use of meta tags for search engine optimisation starts to wane as search engines develop different methods of searching for and ranking search results.

However, the concepts discussed in this article may continue to be instructive when applied to meta data generally. The interactivity of modern web-based applications is giving rise to more and more services that allow subscribers to upload information onto a profile or portfolio which can then be utilised by others who are searching the site, looking to procure goods or services. 'Utilising' in this sense does not mean looking at the profile, as the full profile may be in the form of meta data, and therefore invisible to the user.

The user enters a search term, for example the name of a product or service, and because of terms that the subscriber included in the profile, is directed to a brief entry and a link to the subscriber. The use of product names as part of the profile by the subscriber in this context where the subscriber does not in fact supply those products must qualify as misleading and deceptive conduct, (if not a false and misleading representation such as would found an action under s 53 of the TPA).

To suggest that this type of conduct is acceptable because the average web user knows you can't trust search results on the internet[13] is to settle for mediocrity and a lack of integrity in terms of the internet where the importance of the medium to commerce demands that the same standards be applied to it as are applied in the tangible world of business.

Sponsored links

This article has so far focused on unsponsored links, or 'organic' search results. A recent court settlement suggests that a quick look at sponsored links might be warranted.

Recently, (8 April 2008) Telstra admitted to misleading and deceptive conduct in its Trading Post business organising sponsored links via Google. The background to this litigation is neatly summarised in the ACCC's press release when it launched the case in mid–2007:

> The ACCC is alleging that Trading Post contravened sections 52 and 53(d) of the *Trade Practices Act* 1974 in 2005 when the business names 'Kloster Ford' and 'Charlestown Toyota' appeared in the title of Google sponsored links to Trading Post's website. Kloster Ford and Charlestown Toyota are Newcastle car dealerships that compete against Trading Post in automotive sales.
> The ACCC is also alleging that Google, by causing the Kloster Ford and Charlestown Toyota links to be published on its website, engaged in misleading and deceptive conduct in breach of section 52 of the Act.
> Further, the ACCC is alleging that Google, by failing to adequately distinguish sponsored links from

If the remedy is not to be found under trade marks law, it is likely that the failure to remove the tags will qualify as unlawful misleading and deceptive conduct, depending of course on the overall effect of the conduct …

'organic' search results, has engaged and continues to engage in misleading and deceptive conduct in breach of section 52 of the Act.

Google maintains that the ACCC's claims against it in this litigation are without merit and will continue to defend them vigorously.

Where Trading Post went wrong, of course, is that the relevant trading names appeared in the headlines of the sponsored links, not just in the 'invisible' keyword triggers.

Google has long had a policy in many countries (including Australia) of investigating trade mark complaints by registered owners and, if upheld, disabling the relevant keyword triggers from the ads complained about, but it will not review keyword triggers in the US and Canada, and has recently extended the US and Canada policy to the UK and Ireland.[14]

This policy change appears to be a reaction to the 'Mr Spicy' case recently decided by the English High Court,[15] in which it was held that Yahoo had not infringed the claimant's registered trade mark MR SPICY by allowing a search for 'Mr Spicy' to produce sponsored links to two supermarkets. In that case the keyword used was actually 'spicy' but the court held that Yahoo was not using the mark in the relevant sense and, even if it had been, the trade mark owner's interests were not being affected in the relevant way to support a trade mark infringement. Note the search results did not refer at all to the claimant's business or products.

As part of the policy change, previously disabled keywords in the UK and Ireland will be reinstated (effective 5 May 2008). Google will, however, still investigate complaints against trade mark use in advertisement text (as opposed to keywords) in all these jurisdictions.

Conclusion

Traders who have developed a business reputation, whether in the traditional business world or online, should be able to stop incidences of meta tagging where it infringes the consumer protection provisions of the TPA. If the result produced does not and is not likely to confuse the user, but merely provides them with an alternative source of the goods and/or services to consider, this is something that the trader with the established brand might just have to put up with, whether or not the tags used are registered trade marks.

In paid advertising, such as Google AdWords, the aggrieved trader can still (except in the US, Canada, the UK and Ireland) lodge a trade mark complaint with Google in respect of keywords that are trade marks.

Finally, it is interesting to note that Google itself advises that, apart from paid advertising, 'the best way to ensure a results listing on Google is for many other sites to link to you'. This has become the focus of those wishing to optimise organic search results, rather than relying on meta tagging. ●

Catherine Logan,
Partner,
Hunt & Hunt.

Endnotes

1. *Reed Executive Plc v Reed Solutions Plc* [2002] EWHC 1015.
2. *Reed Executive Plc v Reed Business Information Ltd* [2004] EWCA Civ 159.
3. Above at [148].
4. Above.
5. Above, at [147].
6. Above.
7. *ACCC v Telstra Corp Ltd* [2004] FCA 987; BC200404708.
8. *United Telecasters Sydney Ltd v Pan Hotels International Ltd* (1978) ATPR 40-085.
9. [2003] FCA 536; BC200302768.
10. Above, paragraph 36.
11. *Lanham (Trademark) Act* (15 USC) s 1114.
12. *Trade Marks Act 1995* (Cth) s 122(d).
13. Above n 2.
14. <https://adwords.google.com/support/bin/answer.py?answer=92877&ctx=sibling>.
15. *Victor Andrew Wilson v Yahoo! UK Ltd and Overture Services Ltd* [2008] EWHC 361 (Ch) 68.

Internet Law Bulletin

CASENOTE

Software and copyright: lessons for developers

Michael Pattison and **Margaret Walsh**
ALLENS ARTHUR ROBINSON

In the recent Federal Court case *Dais Studio Pty Ltd v Bullet Creative Pty Ltd*,[1] a software owner was unsuccessful in taking action against a company that was clearly making unauthorised use of the owner's software. The plaintiff lost, even though the software had been obtained by a former employee who had signed an undertaking to protect the company's confidential information. The case serves as a reminder of some basic steps that software owners should take to protect their property.

Facts

Dais Studio Pty Ltd (Dais) began developing a content management system (CMS) known as WebStable (the WebStable CMS) in 1999. The CMS enabled a user to edit the content and appearance of a website online. Mr Petro was employed by Dais as a web developer. After leaving Dais, Mr Petro copied, and made commercial use of, two JavaScript files that formed part of the CMS (the table file and the editor file). The table file allowed a user to change the appearance of a table by re-ordering its entries, while the editor file allowed a user to change the appearance of text.

Dais alleged that in copying and making use of the files, Mr Petro had:

- infringed copyright;
- breached his confidentiality undertaking;
- breached an equitable obligation of confidence; and
- contravened s 183(2) of the *Corporations Act 2001* (Cth).

Subsistence of copyright in source code

Under the *Copyright Act 1968* (Cth) s 10(1), software is protected as a literary work. In order to attract copyright protection, source code must satisfy the definition of a 'computer program'. A computer program is defined to be a set of statements or instructions to be used directly or indirectly in a computer in order to bring about a certain result.

Dais argued that each of the JavaScript files was in itself a computer program. However, it was acknowledged that neither of the files could perform a function in isolation; a result could only be achieved when the files were incorporated into a CMS.

Jessup J held that the current definition, which focuses on bringing about a result rather than performing a particular function as previous definitions had, does not require a set of instructions to bring about a certain result unaided or by its own doing. By analogy, a brake pedal may be said to bring about the result of stopping a car, notwithstanding that the pedal alone would not be able to achieve such a result.[2]

Each file was considered a discrete entity which added functionality to the CMS, and was therefore considered a computer program subject to copyright. It should be noted that each file was considered substantial enough to separately attract copyright protection, despite the small size of the files (a combined total of 497 lines). The arguably insubstantial results achieved by the files was also held not to be an impediment to copyright subsistence.

Infringement of copyright in source code

In order for the copying of a literary work to amount to infringement of copyright, a substantial part of the work must be reproduced. Substantiality is generally a qualitative question. The measure of substantiality will differ between classes of works. In the case of a computer program, the substantiality of what has been taken must be assessed with respect to the originality with which that part expresses the means by which the desired result is brought about.[3] The degree of skill, labour, judgment and expense involved in creating the program should also be considered.[4] In the present case, Jessup J also considered quantitative measures of substantiality. The quantitative measure used was the proportion of lines of code in the whole work constituted by the part reproduced.[5] Ultimately, the table and editor files were not a substantial part of the CMS, and infringement of the CMS could not be made out. However, infringement of the copyright subsisting in the files individually was considered in the alternative.

The issue of infringement of the files individually was complicated by the fact that the WebStable CMS was continuously evolving. Dais's case was conducted on the basis that Mr Petro had infringed copyright in a particular version of the CMS, as implemented in a particular client website. Dais was therefore required to show that Mr Petro had copied the files from that particular version of the software. While Mr Petro admitted that he had copied the files from a Dais website, it could not be shown from which website, and therefore which version of the CMS. As such, no causal link could be established and infringement of copyright could not be found.

If Dais had been able to point to a master version of the software from which subsequent copies of the software were derived, then it may have succeeded, by showing there had been indirect copying of this master version by way of copying from a derivative version. However, indirect copying could not be shown in the case of so-called 'sibling' versions, neither of which was derived from the other.

Protection of source code as confidential information

The source code was found not to be confidential. In making this finding, Jessup J considered the factors set out in the American Restatement of Torts,[6] including:[7]

- the extent to which the information was known both inside and outside the business;
- the ease or difficulty with which the information could be properly acquired or duplicated by others;
- the steps taken by the employer jealously to guard the information; and
- the commercial value of the information.

heard to assert that there was some impropriety in a stranger viewing and absorbing that information and using it to his or her own lawful advantage.[8]

The files copied by Mr Petro were held not to fall within the scope of his confidentiality undertaking. The agreement entered into by Mr Petro on commencement of his employment with Dais claimed to bind him in relation to 'confidential information'. No further definition of this term was given. The court interpreted the agreement narrowly due to the ambiguity introduced by the use of the generic term 'confidential information'.

Implications for software developers

While intellectual property protection is available for computer programs, it will not necessarily be easy to prove that an infringement has occurred. Additionally, it will be difficult to rely

... lack of copyright notices was said to show that Dais had taken no serious steps to protect the confidentiality of the files, despite the inclusion of confidentiality clauses in contracts with clients.

Jessup J considered the fact that many similar files are freely available online and that an identical file could be created from scratch with relative ease to be of particular significance. Jessup J also noted that no copyright or other proprietary notices had been included in the source code. This lack of copyright notices was said to show that Dais had taken no serious steps to protect the confidentiality of the files, despite the inclusion of confidentiality clauses in contracts with clients.

Jessup J also expressed the opinion that if a third party were to acquire the code from a website by using the location and names of the subject files to locate the source code, there would be no impropriety in doing so. It was said that a person who leaves information in a place which, while concealed to a point, is nonetheless accessible to members of the public without breach of the law, cannot be

on the action for breach of confidence to protect source code where such code is used on the internet.

If your client develops software then you should:

- advise that all program files contain a comprehensive copyright notice — in the present case, the lack of copyright notices was successfully used to argue that the source code was not confidential information;
- make sure that software is expressly referred to in the terms of any confidentiality agreements. The court was reluctant to give meaning to ambiguous generic terms and chose to interpret the confidentiality obligations narrowly. The more specific the obligations, the stronger the protection;
- advise clients to retain copies of version releases so that they can be relied on if one of several sub-versions has been reproduced. If a

developer is unsure which derivative version has been copied, an action may succeed based on an indirect copying of the earlier work; and advise that if a program's source code has to be available on the internet for the program to operate, the client should take whatever steps are possible to make that access as difficult as possible. ●

Michael Pattison, Partner, Allens Arthur Robinson, Melbourne,

Margaret Walsh, Research Assistant, Allens Arthur Robinson, Melbourne.

Endnotes

1. *Dais Studio Pty Ltd v Bullet Creative Pty Ltd* [2008] FCA 42; BC200800244.
2. Above n 1 at [31].
3. *Autodesk Inc v Dyason (No 2)* (1993) 176 CLR 300 at 305 per Mason J, approved by *Data Access Corporation v Powerflex Services Pty Ltd* (1999) 202 CLR 1 at 32–33.
4. Such a measure was also used in *Tamawood Ltd v Henley Arch Pty Ltd* (2004) 61 IPR 378 at 389 (as cited by Jessup J in the current case).
5. Above n 1 at [56].
6. At [2007] FCA 2054 at [65] Jessup J considered the factors listed in Art 757 of *The Restatement of the Law of Torts*. In the case of *Ansell Rubber Co Ltd v Allied Rubber Industries Pty Ltd* [1967] VR 37, these factors were held to be relevant in the Australian context. While some cases, such as *Mense & Ampere Electrical Manufacturing Co v Milenkovic* [1973] VR 784 at 796–8, appeared to apply these factors as a rigid checklist, the weight of authority suggests that they are merely relevant lines of enquiry: see *Deta Nominees Pty Ltd v Viscount Plastic Products Pty Ltd* [1979] VR 167 at 193.
7. Above n 1 at [65].
8. Above n 1 at [75].

Legitimising web-based music 'piracy'

Adam Sauer BARRISTER AND SOLICITOR, SUPREME COURT OF VICTORIA

That we are increasingly living in a world dominated by digital technologies is unquestionable. One way this is evident is the digitisation of music made available on the internet. This represents a significant market change. Though record companies have bemoaned the destruction of their traditional ways of disseminating music, digital music has not negated CD sales. However, digital music is fast becoming a viable and enticing alternative, offering cheaper prices and streamlined delivery straight to one's computer. Its format is compatible with various portable music devices, and digitised music files can be burnt to create a CD.

In Australia in 2007, 17.6 million digital tracks were legally downloaded, but only 790,000 digital albums were downloaded compared with the 32 million physical albums that were purchased. In general, digital sales were up 43 per cent in value from 2006.[1] At the time of writing, physical album sales are down by 10 per cent in value compared with 2007 figures, with the shortfall being largely attributed to file sharing and illegal downloads.[2]

Probably the most common way of legally downloading music around the world is through Apple's software program iTunes. The program boasts to 'deliver … anything you want, instantly', from music to movies, from television shows to audiobooks.[3] Actually, there is a limit in relation to music, the focus of this article — iTunes offers (only) over six million songs.[4] This figure is even less in the Australian context as the Australian iTunes store is not as exhaustive as the North American one.

What then of those songs that are not downloadable via iTunes? Some may be downloadable legally through other websites, such as Amazon, Yahoo Music Unlimited or Telstra's BigPond, but these sites generally only provide the popular content that would be found on iTunes. In the absence of legally downloadable music, a consumer may have to hunt out a physical recording. But what if the desired song or album still cannot be located, whether because it is too old, out of print, a rarity, deemed not popular enough to continue production or for any other reason? This is where illegal peer-to-peer music sharing technologies such as Napster (no longer free), Kazaa (now 100 per cent legal) and their newer successors such as LimeWire (mere pretentions of legality but free)[5] can satisfy consumer needs. These technologies, depending on your view, valuably help disseminate culture or are 'vehicles for inducing and facilitating mass infringement of copyright.'[6] This article, despite the legal complications involved, favours the former view. It is argued that it is not morally wrong to turn to such sharing facilities when all else fails in the search for music.

Copyright Act

Copyright in sound recordings is granted under s 89 of the *Copyright Act 1968* (Cth) (the Act) and s 85 sets out the corresponding rights. For the purposes of this article the relevant rights are to make a copy of the sound recording (s 85(1)(a)) and to communicate the recording to the public (s 85(1)(c)). The duration of copyright in a sound recording, under s 93 of the Act, is 70 years after it was first published. Copyright also subsists in the underlying literary work (lyrics) and musical work (s 32). The relevant rights in this instance are to reproduce the work in a material form (s 31(1)(a)(i)), to publish the work (s 31(1)(a)(ii)) and to communicate the work to the public (s 31(1)(a)(iv)). Under s 33(3) of the Act, the duration of copyright in the work is, assuming the work was made public in the creator's lifetime, the life of the creator plus 70 years. Once in the public domain, copyright in a work cannot be resurrected. However, a consumer must wait a long time for a work to be freely available in the public domain. Though this article does not intend to discuss the role of ISPs or those behind peer-to-peer systems, it is worth noting that they may be liable under s 101(1A) of the Act for authorisation of copyright infringement.

With the Act in mind, lawyers and clients should remember that everything about a peer-to-peer provider such as LimeWire potentially infringes the copyright holder's rights — initially ripping music from a CD, uploading or downloading pirated music and making music available to download from your computer via a peer-to-peer system. The fair dealing provisions[7] of the Act are limited to exclude even the right to make a back-up copy of a CD legally purchased, including transforming it into an MP3 file on your computer, unlike in the US which has free use provisions. To take it further, though the wider implications are beyond the scope of this article, a blanket prohibition on peer-to-peer providers may lead to litigation over programs such as iTunes, Windows Media Player and Nero which enable CD burning and, in the case of the first two, ripping and conversion to digital music files.

Copyright owners v utilisation and growth of culture

In the instance of rare, obscure or out-of-print songs — and this is largely what I am discussing here — one may ask, 'what is the financial imperative for copyright owners to crack down on those who provide access to and download the files?' In some cases, works of art are intended to be limited; for example, numbered editions of books, pieces of performance art or limited box edition music. But if a piece of music has simply been deleted from the record company's active production list, then where is the harm in downloading it? Clearly the company is not seeking to reap further financial reward from the piece if they are no longer releasing it.

> … if a piece of music has simply been deleted from the record company's active production list, then where is the harm in downloading it? Clearly the company is not seeking to reap further financial reward from the piece if they are no longer releasing it.

I am not talking about small numbers here. Lawrence Lessig notes that 'by one estimate, 75 per cent of the music released by the major labels is no longer in print'[8] (it does not require much thought to come to the conclusion that this is solely for economic reasons) and, one may assume, legally inaccessible or at least very hard to obtain. The point that more digital files could be made legally available for a fee was acknowledged by Wilcox J in his summary of *Universal Music Australia Pty Ltd v Sharman Licence Holdings Ltd*[9] (*Sharman*).[10] His Honour further stated that the applicants' remedies in copyright would be limited and, giving hope to dealers in digital music on the internet, that that the applicants were 'entitled to protect… [their] copyright… [but] not entitled to control the internet.'[11]

It is argued that copyright holders, usually record companies, only become concerned about illegal downloading and seek legal redress when it looks to impact on their profits. For example, the fan website 'Elliott Smith B-Sides & Other Songs'[12] had for years posted otherwise impossible to obtain demos, unreleased songs and rare b-sides by the late singer Elliott Smith. In April

2007, the copyright holders demanded the take-down of various songs and a number of these songs surfaced on the posthumously released double album *New Moon* (2007). Other songs are yet to appear commercially but we may anticipate they will. Without wanting to name names, it is worth noting that there are sites that offer much of what was taken down from 'Elliott Smith B-Sides & Other Songs'. The irony is that Elliott Smith was open to fans sharing his music (illegally) across the internet, which goes to show it is important to note where the copyright and control lies.[13]

Record companies argue illegal downloads are akin to stealing and deprive them and creators of profits. Maybe so, but it is worth keeping in mind that by and large most people are not making a profit from sharing music. For otherwise unobtainable music that is *shared* rather than sold, while it may involve a breach of copyright, there is no effect on profit. We may ask, 'is this enough to distinguish this type of sharing from true piracy?' Lessig likens the sharing of out of print music to purchasing items from used book or record stores, a purchase which does not provide the artist or copyright holder with any money. Lessig facetiously posits that if file sharing is to be stopped, then surely libraries and used book and record stores must be closed down.[14] Like these other cultural artifacts, music has the potential to go on to have a 'second life' after it has been essentially discarded by the copyright holders, a life which is 'extremely important to the spread and stability of culture.'[15] But unlike books in libraries, where the copyright holder does not continue to make a profit no matter how many times a book is read, though money is collected by educational and Public Lending rights schemes and thus there can be a second (economic) life in books, in the case of music 'there is no guarantee of a second life … it is as if we've replaced libraries with [stores and] … what's accessible is nothing but what a certain limited market demands. Beyond that, culture disappears.'[16] It is through peer-to-peer sharing that music can be given its second life. This kind of sharing is 'good for society (since more exposure to music is good) and harmless to the artist (since the work is not otherwise available).'[17] A similar philosophy is espoused by Christian Slater's character in *Pump Up the Volume* (1990), who runs a pirate radio channel for an enthusiastic audience of fellow teens by 'stealing' bandwidth. He states: 'I'm calling for every kid to seize the air. Steal it, it belongs to you ... Keep the air alive.'[18]

Culturally justifying illegal downloads

To justify turning to illegal download sites we may look to the history of Western artistic creation. Lessig argues:[19]

> We come from a tradition of 'free culture' … [which] protects creators … directly by granting intellectual property rights … [and] indirectly by limiting the reach of those rights, to guarantee that follow-on creators and innovators remain *as free as possible* from the control of the past.

That is, culture builds upon culture. Lessig goes as far as to say that 'if "piracy" means using the creative property of others without their permission' and if the notion that if something created is of value then the creator has rights is true, 'then the history of the content industry is a history of piracy.'[20] That is, big media has developed in a free culture that has allowed it to borrow from and build on the past. In the majority of cases, in today's free culture, if indeed we still operate in one, laws prohibiting the illegal sharing of music arguably have nothing to do with protecting the rights of creators but those of the corporations that hold the copyright. Record companies seek to enforce this culture with the buying or denying paradigm and one which illegal peer-to-peer systems buck firmly against.

Making digitised music more readily available

One problem with legitimising peer-to-peer file sharing is that it would be impractical, if not impossible, to distinguish between those downloading illegal music because they do not wish to pay and those for whom there is no other option for accessing the music. In the US case *MGM Studios v Grokster Ltd*, the applicants' submission contained the statement that the 'defendants have created a 21st century piratical bazaar'.[21] No doubt there are both types of content seekers downloading music.

One solution is for the copyright holders to become online distributors themselves or at least make the songs available electronically. Online stores such as iTunes are an example of this. Kazaa in its submissions in *Sharman* purported to 'have offered copyright owners the ability to protect, promote and sell their works to millions of users. Everything is in place. They just need to try it.'[22] Kazaa further submitted: 'If peer-to-peer provides a bigger market, lower costs and unlimited space in packaging music… [if] these companies tried it, they could make so much more [money]. They need to stop fighting this technology and start working with it.'[23] This approach would in theory only penalise true pirates: those who just want something for free. Given the time that has passed in which record companies could have done so, it is

For otherwise unobtainable music that is shared rather than sold, while it may involve a breach of copyright, there is no effect on profit.

doubtful that back catalogues will be appearing online any time soon — it is a simple supply and demand equation. There has been reluctance on behalf of record companies to directly release digital music, or find a viable alternative to satisfy consumer demands to have music available

> MIPI reports that in Australia approximately 2.8 million individuals, or 18 per cent of the population, download music illegally through file sharing networks every year, with each individual downloading on average about 30 songs per month.

instantly. Innovatively, the pre-order package of the new Portishead album *Third* (2008) comes in a package with a vinyl copy of the album and a data stick containing a digital copy of the album. Prior to the release of the White Stripes' latest album *Icky Thump* (2007) the band released limited edition data sticks containing the album in digital form. The impetus in both cases seems to have come from the bands rather than the record companies, appealing to the fans' desire for digital music (but not escaping charging a fee). Further, it must be noted that in the case of both artists the albums can be downloaded from iTunes.

Australian litigation

Music Industry Piracy Investigations (MIPI) reports that in Australia approximately 2.8 million individuals, or 18 per cent of the population, download music illegally through file sharing networks every year, with each individual downloading on average about 30 songs per month.[24] This is clearly enough to put record companies on guard. However, as at February 2008, the Australian Copyright Council notes that 'at least three' individuals have been prosecuted for illegal file sharing, while a provider of peer-to-peer software settled out of court with record companies.[25] There is clearly a discrepancy between illegal acts in this instance and prosecution of these. Indeed, 'the music industry in Australia … would prefer not to [sue individuals for illegal file sharing].'[26] According to Sabiene Heindl of MIPI , the music industry prefers to collaborate with ISPs, believing 'ISPs should take appropriate responsibility for protecting [online music content]' as they 'play a very significant role in the chain of online content distribution.'[27] Further, it is in their interests to take a more active role in order to avoid prosecution for copyright authorisation and to minimise the network congestion caused by file sharing.[28] What is more, with peer-to-peer providers scattering their assets among various jurisdictions, the ISP is often the easiest target to prosecute.

It can be difficult to prosecute the actual file sharing systems, such as Kazaa and LimeWire, because the servers are usually decentralised, capable of running without direct human input and may function through corporations, individuals and technologies scattered across numerous jurisdictions. In the case of prosecuting individuals, while this has been vigorously pursued in the US,[29] in Australia the attitude seems to be that the impact is not sufficient to bother. It may even be argued that the courts and legislators are inappropriate governors of the internet. The circumstances in which the internet has developed and its very nature mean online social norms and technology play more of a role in shaping online behavior than the law, which in fact lags behind technology.[30]

The watershed case in relation to file sharing in Australia is *Sharman* which dealt with the peer-to-peer facility Kazaa. The facility was a jurisdictional mess. Although the company had assets across the globe,[31] the case was initiated in Australia, presumably because Sharman Networks Ltd (second respondent), run under the Australian management company LEF Interactive (third respondent) the sole director and shareholder of which was an Australian citizen (fourth respondent), operated the website. The other respondents, individuals and organisations, were affiliated with Sharman Networks in one way or another. Wilcox J found six of the 10 respondents knew Kazaa was being used to illegally share copyrighted files. Further, while there were technical measures which could have been taken to reduce the number of copyrighted files traded, none were implemented. Conversely the respondents actively promoted illegal trading and thus had, in contravention of s 101 of the Act, authorised users to do unauthorised infringing acts with copyrighted material in Australia. The respondents were also found to have entered into a common design with one another to carry out, procure or direct the authorisation.

In a non-draconian manner, Wilcox J noted that the respondents needed to be allowed time to modify their system so as copyright was not infringed — he did not want to curtail 'others' freedom of speech and communication.'[32] An injunction was ordered preventing the named respondents from authorising users of Kazaa to do any infringing acts in Australia. Essentially, Kazaa was not prevented from running, so long as it complied with the orders restricting its contraventions of the Act.

Advice to clients

After *Sharman*, if advising clients who wish to operate a similar peer-to-peer file sharing system, the most watertight advice would be not to. Knowledge that illegal trading is operating and even promoting such trading will not work in the client's favour. Similarly, if the client has access to technology that can restrict the number of illegally traded files, such technology should be implemented. The presence of a disclaimer to the effect that it is illegal to trade in copyrighted music without a licence from the owner and that users are to refrain from using the sharing system for illegal purposes, such as LimeWire presents its users now or as Kazaa did, will likely be ineffective to avoid prosecution — especially if there is knowledge that illegal sharing is going on. Further, as an antecedent to any trial, Anton Pillar orders may be issued to determine an individual's or organisation's role in any illegal file sharing. More slyly, we can also interpret from the judgment in *Sharman* that it may be favourable for the client, and create difficulties for the court, if knowledge is spread such that no one person can be said to be in control of the system or have full knowledge of it or its source code. This makes it harder to point the finger.[33] Similarly, to create jurisdictional complications it may be prudent to spread assets (servers, software and the like) across numerous jurisdictions (as of September 2005, Vanuatu provided sturdy protection and veils of secrecy to owners of corporations incorporated in the island). Avoiding a central server with the details and habits of every user would also be beneficial because it could go toward denying knowledge of illegal activity.[34]

Conclusion

It may be that the benefits of illegal peer-to-peer sharing outweigh the detriments if it means the continual exposure to otherwise unobtainable music and the continuance of a free culture. Writing as a consumer and not a producer of music or the copyright owner of music, I am in favour of peer-to-peer file sharing systems that allow one to download otherwise unobtainable songs.

However, we have seen in *Sharman* that a Kazaa-style free illegal download system will not stand in Australia; this is why record companies need increasingly to make music digitally available. The legal rights of creators and copyright owners cannot be ignored and lawyers must be aware that clients who engage in illegal file sharing are breaching copyright. A balance should be struck between the demands of consumers and the rights of creators and copyright owners.

One way to do this would be for record companies to be more willing to release back catalogues as online music files. This article has as its intended focus songs that are not obtainable from legal sources. If there is *no option* to purchase particular songs in the first place then it is arguable copyright holders are putting unreasonable strictures on culture. There is no economic imperative in preventing the download of songs the copyright holders do not intend to sell in the first place. With the barriers nonetheless in place, it may indeed be time to start 'stealing' music to keep it 'alive'. ●

Adam Sauer,
Barrister and Solicitor,
Supreme Court of Victoria.

The author would like to thank Ian Cunliffe for the initial idea for the article, Dr Melissa deZwart for her direction to sources of information and Happy Harry for inspiration.

Endnotes

1. Australian Recording Industry Association Ltd., *ARIA Releases 2007 Wholesale Music Figures* (2008), Australian Recording Industry Association at <www.aria.com.au/pages/ARIAreleases2007wholesalemusicsalesfigures.htm> accessed 14 April 2008.

2. Burns A 'Slipped disc hurts industry', *MX* (Melbourne) 14 April 2008, 7. For further figures on the impact of illegal downloads on the music industry see Heindl S 'Gone for a song: illegal file sharer fined $US220,000' (2007) 10(7) *INTLB* pp 88–9.

3. Apple Inc., *iTunes Overview* (2008) at <www.apple.com/itunes/overview/>, accessed 14 April 2008.

4. Apple Inc., *iTunes Store* (2008) at <www.apple.com/itunes/store/> accessed 14 April 2008.

5. On its official site, LimeWire states 'LimeWire is legal software, but it is illegal for you to use LimeWire to share copyrighted files without permission…When you download LimeWire software…you agree to refrain from using LimeWire for the purpose of copyright infringement.' (Lime Wire LLC, *Copyright Information* (2008) at <www.limewire.com/about/copyright.php>, accessed 7 March 2008.) Surely the makers of LimeWire are aware that the vast majority of file sharing over their system is illegal and if an Australian court were to follow *Universal Music Australia Pty Ltd v Sharman Licence Holdings Ltd* (2005) FCA 1242; BC200506481 it is likely an Australian-based facility with the same disclaimer would be found liable for authorising the infringement of copyright by another under s 101 of the Act.

6. Heindl above n 2 p 88.

7. See the *Copyright Act (1968)* (Cth) Pt III Div 3 for the fair dealing provisions.

8. Lessig L *Free Culture* (2004) p 314 n 15. Available at </www.free-culture.cc/>.

9. With corrigendum dated 22 September 2005 [2005] FCA 1242; BC200506481.

10. Above.

11. Wilcox J in Davidson J 'Win or Lose, Kazaa Won't Be Shut Down' *Australian Financial Review* 3 December 2004 p 64.

12. <www.elliottsmithbsides.com/index2.html> accessed 9 March 2008. Note: this website is no longer accessible.

13. Ramirez C *Frequently Asked Questions* Sweet Adeline <www.sweetadeline.net/faq.html> accessed 12 April 2008.

14. Above n 8 p 72.

15. Above n 8 p 113.

16. Above.

17. Above n 8 p 69.

18. New Line Cinema, *Pump Up the Volume* (1990).

19. Above n 8 p xiv.

20. Above n 8 p 53.

21. 545 US (2005), MGM Studios et al., Complaint for Damages and Injunctive Relief for Copyright Infringement (2 October 2001) p 2

22. *Universal Music Australia Pty Ltd v Sharman Licence Holdings Ltd* [2005] FCA 1242; BC200506481 at 83.

23. Above.

24. Music Industry Piracy Investigations, *What is Music Piracy?* (2006) <www.mipi.com.au/musicpiracy.htm> accessed on 24 March 2008.

25. Australian Copyright Council, *Internet: Copying and Downloading Material* (2008) p 4 at <www.copyright.org.au/publications/G056.pdf> accessed 23 March 2008.

26. Heindl above n 2 p. 89.

27. Above.

28. Above.

29. Heindl estimates 'over 20,000' cases have been brought against individual file sharers by record companies in the US (Above n 8 p 88).

30. See, for example, Lessig L *Code and Other Laws of Cyberspace* (1999) and Sauer A 'Protecting the Copyright Balance in Cyberspace' (2007) 12 *Media & Arts Law Review* p 239.

31. The domain name was registered in Australia and the company running the site was in Australia, the servers were located in Denmark, the software in Estonia, the company was incorporated in Vanuatu and users were worldwide. To avoid the ramifications of litigation against it in Denmark, in 2002 the company Kazaa BV transferred ownership to Sharman Networks of the website, the domain name and the necessary software for users to trade songs. Later the software driving this was transferred via an irrevocable licence by a related body.

32. Wilcox J 'Summary' in *Universal Music Australia Pty Ltd v Sharman Licence Holdings Ltd* [2005] FCA 1242; BC200506481.

33. Above, see Wilcox J's remarks at 24 and 25.

34. Above n 32 at 195–211.

bytes

US releases discussion paper on a possible anti-counterfeiting trade agreement

At the July G8 meeting in Tokyo, members will discuss a new multilateral treaty proposed by the US, called the Anti-Counterfeiting Trade Agreement (ACTA). The ACTA includes a broad range of new measures designed to protect against IPR (and especially copyright) infringement.

Central to ACTA is an attempt to create new, uniform measures to combat piracy. It proposes that there be increased co-operation internationally between law enforcement agencies and customs officials.

A key element of the proposal includes the introduction of broad new powers for border guards, who would be entitled to search any electronic device for material that infringes copyright. The guards would also be empowered to address any infringement, including by destroying infringing material or confiscating the device altogether.

The ACTA would also address infringement over the internet by creating new 'safe harbour' provisions for ISPs. In return, the ACTA contemplates that ISPs would be required to provide the details of individuals identified as potentially infringing intellectual property rights.

In addition, the ACTA would establish a new body to govern copyright protection at an international level, as well as introducing criminal penalties for various infringement and trafficking activities.

Interestingly, rights under the ACTA would be enforceable by parties other than the particular rights holders in each instance and, if implemented, would mark a new chapter in the efforts of legislators to protect content in the internet age. ●

Alex Hutchens,
Lawyer,
Blake Dawson.

BOOK REVIEW

Superhighway Robbery: Preventing e-commerce crime

Graeme R Newman and Ronald V Clarke
Willan Publishing distributed by Federation Press
ISBN: 978 1843920182
RRP $80

Review by Sharon Givoni GENERAL EDITOR

While e-commerce has introduced enormous efficiencies into the marketplace, it has brought with it vast new opportunities for criminals, making it easier to crime commit internationally and impact on millions of victims at one time.

In their new book *Superhighway Robbery*, Newman and Clarke provide an analysis of the crime opportunities offered by the internet and e-commerce. Rather than explore the cause of such crime in any detail, the focus of the book is how our understanding of the nature of the crimes can be applied to *prevent* further online crime and reduce victimization.

The book seeks to identify the specific opportunities and transactions in which crime can occur in the e-commerce environment, and the different kinds of information which are targets for crime. Intellectual property, intelligence, information systems and services of various kinds (such as banking and purchasing), extortion, terrorism, fraud, theft and computer crime are all discussed.

Consumer products are also examined with a view to identifying the elements that make them particularly vulnerable to theft. Topics covered include:

- situational crime prevention in the information society;
- basic features of e-commerce;
- customer identity;
- monitoring, tracking and surveillance;
- globalisation; and
- the e-commerce value chain.

According to the authors, one of the main things that came out of writing the book was how easily the body of research on situational crime prevention could be applied to preventing cybercrime.

'It is pretty obvious that information is the prime target, truly a "hot product" and that the internet environment and technologies are great tools that make getting our work done more efficiently and that applies to criminals too', they comment when interviewed by the reviewer. Two important lessons they learned from writing the book are that:

- most cyber-crime is committed by ordinary individuals without any special hi-tech computer skills; and
- human error is the main cause of cyber-related crime, so standard crime prevention techniques apply, especially in the context of training of private sector employees.

They were also surprised by how easily the body of research on situational crime prevention could be applied to preventing cybercrime. ●

PUBLISHING EDITOR: Alison Hartman PUBLISHING OPERATIONS MANAGER: Anupama Bhattacharya PRODUCTION: Christian Harimanow
SUBSCRIPTION INCLUDES: 10 issues per year plus binder SYDNEY OFFICE: Locked Bag 2222, Chatswood Delivery Centre NSW 2067 Australia
For further information on this or other LexisNexis products, call Customer Relations: 1800 772 772 Monday to Friday 8.00am-6.00pm EST;
email: customer.relations@lexisnexis.com.au; or visit www.lexisnexis.com.au for information on our product catalogue.
Editorial enquiries: alison.hartman@lexisnexis.com.au

ISSN 1329-9735 Print Post Approved PP 244371/00049 Cite as (2008) 11(3) *INTLB*