COMPUTERS & LAW

Journal for the Australian and New Zealand Societies for Computers and the Law

Editors: Nicole Wellington, Belinda Justice and Claire Elix

ISSN 08117225

Number: 55

March 2004

Peer-To-Peer Filesharing Networks: The Legal and Technological Challenges for Copyright Owners

Nicholas Blackmore, Corrs Chambers Westgarth

Nicholas Blackmore is a solicitor in the Information Technology group at Corrs Chambers Westgarth in Melbourne. He advises on a range of technology-related legal issues, including procurement, outsourcing, electronic commerce, intellectual property and privacy. He is also a committee member of the Victorian Society for Computers and the Law.

1 Introduction

When Shawn Fanning created Napster in 1999 as a way of helping his fellow college students find difficult to locate MP3 files on the Internet, he could scarcely have imagined that Napster and other peer-to-peer filesharing software would become as important a technological advance as the MP3 file format itself.[1] Today, the recording industry estimates about 2.6 billion songs, movies and other works are shared through peer-to-peer filesharing networks. A high proportion of these works are shared without the consent of copyright owners.

In the United States, there have been two high profile cases against operators or creators of peer-to-peer filesharing networks alleging copyright infringement. The first of

Continues page 3

In this issue:

Continued from page 1

these was *A & M Records, Inc v Napster, Inc*,[2] a case brought by plaintiffs representing a large number of recording studios and artists. In that case, the District Court for the Northern District of California held Napster liable for contributory and vicarious copyright infringement. The decision was upheld on appeal.[3] At the time, the *Napster* decision was hailed as 'shout[ing] out that copyright protection [was] alive and well even in cyberspace'.[4]

Several years on, however, the victory for copyright owners in *Napster* began to look decidedly pyrrhic as new filesharing networks like Gnutella and FastTrack, which were structured to avoid the features identified by the courts in *Napster* as giving rise to liability, began to gain popularity. In *MGM Studios Inc v Grokster Ltd*,[5] another case brought by plaintiffs representing movie studios, recording studios and artists, the District Court for the Central District of California held that neither Grokster Ltd, a distributor of the FastTrack-based Grokster software, nor StreamCast Networks Inc, a distributor of the Gnutella-based Morpheus software, were liable for contributory and vicarious copyright infringement. The plaintiffs in Grokster are now left considering their legal and technological options to stem the flow of copyright infringement which they claim is costing them billions of dollars each month.

This article discusses the impact of peer-to-peer filesharing networks on copyright law in the US and Australia and examines potential solutions to the problem of copyright infringement over peer-to-peer filesharing networks. This article briefly describes next-generation peer-to-peer filesharing networks and their legally significant features and considers the liability of users of next-generation peer-to-peer filesharing software for copyright infringement committed using that software. This article also considers the liability of distributors of next-generation peer-to-peer filesharing software for copyright infringement committed by users using that software and discusses other legal and technological solutions to the problem of copyright infringement over next-generation peer-to-peer filesharing networks.

2 What are next-generation peer-to-peer filesharing networks?

2.1 Peer-to-peer filesharing networks generally

A computer network is any group of computers connected together which share data. Each computer on the network is referred to as a 'node'.

In a peer-to-peer network, the data available on the network is distributed amongst all nodes on the network. There need not be any node that is 'central' to the network. Each node simultaneously acts as both a client, by requesting data from other nodes, and a server, by serving data to other nodes. While not as efficient or scalable as client-server networks, peer-to-peer networks may be decentralised and incorporate many redundant links and are typically used where an open, robust network is required. The Internet itself is an example of a large peer-to-peer network.

Filesharing peer-to-peer networks vary in architecture, but all share a few common features. First, all peer-to-peer filesharing networks require users to install software on their computer which installs the user interface and connects that computer to the network as a node. Second, all peer-to-peer filesharing networks allow users to elect to make designated files stored on their computers available to other network users upon request – for example, by placing those files in a 'shared folder'.

Third, most peer-to-peer filesharing networks allow users to search the network for files they would like to obtain. The method by which this search is conducted differs between networks. Finally, all peer-to-peer filesharing networks transfer shared files upon request directly from the computer on which that file resides to the requesting user's computer, without intervention by the operator of the network or any third party.

2.2 Next generation peer-to-peer filesharing networks

'Next-generation' peer-to-peer networks are those which have arisen since the demise of Napster, the first widely popular network for sharing music in MP3 format. Napster operated as a centralised network, which was a key factor in its downfall. The next-generation peer-to-peer filesharing networks involve varying degrees of decentralisation. The differences in each architecture are legally significant.

2.2.1 A centralised architecture - Napster

The Napster filesharing network was not a 'true' peer-to-peer network, in that the architecture of the Napster network was based around a central server operated by Napster, Inc. This central server contained an index of all of the shared music files made available by users of the network and details of the locations of those files. Because this centralised index needed to be able to reliably specify the location of shared files, the central server also contained a list of all users of the Napster software, each of whom were issued with a unique username. Nevertheless, Napster was generally described as 'peer-to-peer' because shared music files remained on the Napster users' computers and were not copied to Napster's central server at any time, and file transfers took place directly between users on the network and did not involve the centralised server.

When a Napster user searched for a particular music file, the Napster software would access and search the centralised index and identify the location of any files which matched the search criteria. Accordingly, the central index enabled users to locate music files made available by other users. Without the central server operated by Napster, Inc, the network would cease to function.

Before Napster, many web sites which made copyrighted MP3 files available to Internet users had been found liable for copyright infringement. The peer-to-peer nature of Napster's network architecture represented an attempt to

facilitate identification and sharing of MP3 files, while avoiding liability for infringement of copyrighted music files because Napster itself did not directly copy music files or make those files available to the public.

2.2.2 A partially decentralised architecture – FastTrack

FastTrack is peer-to-peer filesharing software which underlies a number of next-generation peer-to-peer filesharing software products, including Grokster and KaZaA. All FastTrack-based software connect to a common network. The FastTrack-based network is considerably more decentralised than Napster and, as a consequence, distributors of FastTrack-based software have much less control over their users than Napster.

Unlike Napster, the FastTrack network does not feature a centralised server, a centralised index of shared files or a centralised list of usernames. Instead, the FastTrack network employs a system of 'supernodes', which are nodes with heightened functionality. FastTrack software automatically detects the speed with which the computer upon which it is installed is connected to the network and, if that speed is sufficient, will automatically designate that node a supernode. Supernodes are dynamic – a node may be automatically promoted or demoted as a supernode as network conditions change.

The supernodes in the network effectively act as local indexes – they store information regarding files available on nearby nodes and the locations of other supernodes nearby. When a FastTrack user searches for a shared file, the FastTrack software first identifies the nearest supernode – either through a list programmed into the software or from previous searches – and passes the search query to it.[6] The supernode identifies any matches with its local index and passes the search onto other nearby supernodes, which do the same. The search gradually propagates through the network. Search results are returned with details of the location of the file.

While not as efficient as a centralised index, this partially decentralised model has the advantage that the distributor of the software has no control over, or knowledge of, the activities of users on the network and thus is further removed from any copyright infringement engaged in by those users than the network operator is under a Napster-style network – an exception being that most distributors of FastTrack-based software maintain minimal, automated contact with users through 'adware' (software which displays advertisements to the user which may be updated by the creator from time to time) and 'spyware' (software which collects demographic information about the user over time and sends that information to the creator).

This lack of control by the distributor is evident in a number of respects. Because filesharing takes place over the FastTrack network without the assistance of a central server, distributors of FastTrack-based software have no way to track file transfers taking place over the network. It also means that there is no central location at which files can be 'filtered' to block copyrighted or other undesirable content from the network. The absence of unique usernames makes it impossible for distributors of FastTrack-based software to ban particular users, or even to prevent access by users using 'cracked' versions of their software. Many users of the FastTrack network use a cracked version of KaZaA, KaZaA Lite, which provides the same functionality as KaZaA but without the adware or spyware components upon which KaZaA relies for its revenues.

However, users of the FastTrack network are not anonymous – it is relatively simple to identify the Internet Protocol address of a particular node, identify the Internet service provider responsible for that address, and thereby ultimately identify the user.

2.2.3 Wholly decentralised architecture – Gnutella

Gnutella is a 'true' peer-to-peer filesharing network in the sense that it does not involve any centralised server or supernodes. The Gnutella software is open source and is available in a number of versions, including a commercial product called Morpheus. All versions of the Gnutella software connect to a common network.

Gnutella is similar to FastTrack in that it does not feature a centralised index of files on the network or a centralised list of usernames. However, the Gnutella network differs from the FastTrack network in that it does not feature 'supernodes', and accordingly is even more decentralised than the FastTrack network.

When a Gnutella user searches for a shared file, the Gnutella software identifies the nearest three or four nodes on the network and passes the search query to them. Each of these nodes identify any matches with the files stored on those nodes and passes the search onto three or four other nodes on the network, which do the same. The search gradually propagates through the network. Search results are returned with details of the location of the relevant shared files.

Because searches propagate three or four nodes at a time, the Gnutella network is far less efficient than the FastTrack network, but has the advantage that distributors of Gnutella-based software have absolutely no control over or knowledge of the activities of users on the network and thus are very far removed from any copyright infringement engaged in by those users. By not having 'supernodes', the Gnutella architecture also eliminates the potential for supernodes to be targeted in legal proceedings.

3 Liability of users for copyright infringement committed over peer-to-peer filesharing networks

3.1 US copyright law

The courts in *Napster* and *Grokster* had little trouble establishing that users of the respective networks would infringe copyright if they used the network to download or upload copyrighted works.

The Court of Appeal in *Napster* held

that by uploading copyrighted works, Napster users infringed the plaintiffs' exclusive right under the US Copyright Act[7] to distribute the works and by downloading copyrighted works, Napster users infringed the plaintiffs' exclusive right to reproduce the works.[8] The court in *Grokster* agreed with this analysis.[9]

3.2 Australian copyright law

In relation to direct infringement by users of a filesharing network, the Australian law is quite similar to the US position in *Napster* and *Grokster*.

Under Australian copyright law, owners of copyright in literary, dramatic, musical and artistic works have the exclusive right to reproduce their works in a material form.[10] A reproduction is a copy which has some resemblance or objective similarity to the work and was created by actual use of the copyright work.[11] It has been established that a work stored on a computer disk is 'in material form'.[12]

Copyright in a cinematograph film or a sound recording may be infringed by making a copy of it.[13] A copy of a cinematograph film is 'any article or thing in which the visual images or sounds comprising the film are embodied'.[14] A 'copy' of a sound recording is a recording 'embodying a sound recording or a substantial part of a sound recording ... derived directly or indirectly from ... the sound recording'.[15]

Owners of copyright in literary, dramatic, musical and artistic works, sound recordings and cinematograph films also have the exclusive right to communicate their work to the public.[16] 'Communicate' is defined as making available online or electronically transmitting (whether over a path, or a combination of paths, provided by a material substance or otherwise) the work or other subject matter.[17]

Under these provisions, it is clear that when downloading or uploading a copyrighted literary, dramatic, musical and artistic work, cinematograph film or sound recording, users of a filesharing network infringe one or more exclusive rights of the copyright owner.

3.3 Practical considerations

Legal action against users of peer-to-peer filesharing software who infringe copyright is clearly possible under existing law. The reasons that this option has not been widely pursued by copyright owners to date are practical. However, this seems to be changing in the wake of *Grokster* – the Recording Industry Association of America ('**RIAA**') have been identifying peer-to-peer filesharing network users sharing large volumes of copyrighted material with a view to legal action.[18]

The economic feasibility of these actions is probably the biggest obstacle. Finding users who are sharing a sufficient volume of copyrighted works to make it worth pursuing a legal action against them is becoming increasingly easy. A heavy user could comfortably download 60 gigabytes a month over a moderately fast broadband Internet connection, which represents approximately 12,000 songs. The real obstacle to this type of action is the volume of legal actions which would need to be undertaken to make an appreciable dent in the usefulness of a peer-to-peer filesharing network. While some sources suggest that up to 70% of peer-to-peer network users do not share any files at all, even pursuing the top 1% of filesharers currently on the FastTrack network alone would represent 36,000 legal actions.

Targeting this number of users may reduce the efficiency of the FastTrack network by removing the most important supernodes – although others would quickly replace them – but would have less effect on the Gnutella network, which does not feature supernodes. Of course, the chilling effect of just a few hundred high profile prosecutions could be significant in discouraging hundreds of thousands of other filesharers, but one suspects that any attempt to take legal action against users will ultimately be an exercise in futility for copyright owners.

4 Liability of distributors of next-generation peer-to-peer filesharing network software for copyright infringement committed by users

4.1 US copyright law

Under US copyright law, there are two heads under which a person who does not directly engage in copyright infringement may nevertheless be liable for copyright infringement: contributory infringement and vicarious infringement.

In *Napster*, the District Court for the Northern District of California held Napster liable for both contributory and vicarious copyright infringement. The decision was upheld on appeal.[19]

In Grokster, the District Court for the Central District of California held that neither Grokster Ltd nor StreamCast Networks Inc were liable for contributory or vicarious copyright infringement. While the plaintiffs in Grokster have indicated that they will appeal, the decision appears to be fairly soundly based on relevant precedent, in particular the decision of the Supreme Court in Sony Corporation of America v Universal City Studios, Inc.[20]

4.1.1 Contributory infringement

Under US copyright law, a person will be liable for contributory infringement if that person: (a) has actual or constructive knowledge of a direct infringement by a third party; and (b) induces, causes or materially contributes to that infringing conduct. 'Constructive' knowledge in this context means general knowledge that users of the network were engaging in infringing activities – as opposed to 'actual' knowledge of specific incidents of direct infringement.

(a) Napster

The District Court in *Napster* held that Napster, Inc, had both actual and constructive knowledge of direct

copyright infringement by users.

There was considerable evidence that Napster, Inc had actual knowledge of specific acts of infringement – for example, Napster, Inc had been notified by the plaintiffs of approximately 12,000 copyrighted works on the network, and on the basis that a Napster, Inc inter-office memo referred to the need to remain ignorant of users' details 'since they are exchanging pirated music'.

The court held that Napster, Inc materially contributed to the infringing activities of its users by making its software and services available to those users. The court analogised that Napster, Inc was like an organiser of a swap meet who provides premises, parking and advertising to facilitate the sale of counterfeit recordings by swap meet vendors. Although Napster users might be able to share copyrighted works without Napster, the Napster network contributed to the infringing activities by greatly increasing the ease of doing so.

(b) Grokster

The District Court in *Grokster* held that the defendants had both actual and constructive knowledge of direct copyright infringement by users. However, the court refined the analysis in *Napster* when considering the issue of actual knowledge.

The court held that, although there was substantial evidence that Grokster Ltd and StreamCast Networks Inc had actual knowledge of infringement by users – for instance, they had each received notice from the plaintiffs that there were thousands of infringing files being traded on the networks – actual knowledge was only relevant to contributory liability if that knowledge was gained at a time when the defendants were in a position to prevent those acts of infringement. The court analogised to the law concerning a landlord's liability for infringing acts of a tenant. Several US cases have held that a landlord is not liable for infringing acts of a tenant unless the landlord had actual knowledge of those acts at or before the time the landlord signed the lease. Knowledge gained after this time should not give rise to liability because the landlord would be powerless to prevent that infringement.

Accordingly, the court held that any actual knowledge that Grokster Ltd and StreamCast Networks Inc had was irrelevant to the question of liability because that knowledge would inevitably be gained after the software was beyond the control of those parties.

On the issue of constructive knowledge, the court applied the doctrine in the *Sony* case. *Sony* involved the sale of video cassette recorders (**'VCRs'**) by the defendant. The plaintiffs sued the defendant for contributory and vicarious infringement on the basis that the defendant knew that VCRs were likely to be used by consumers to infringe copyrighted television broadcasts. The court in *Sony* held that although the defendant knew as a general matter that consumers might use VCRs for infringing purposes, this 'constructive' knowledge was not sufficient to give rise to liability for contributory infringement provided that VCRs were capable of 'substantial non-infringing uses'.

In *Grokster*, it was undisputed that the Grokster and Morpheus software were capable of substantial non-infringing uses – for instance, distributing non-copyrighted works and distributing works with the consent of the copyright owner. It is worth noting that while these are clearly uses to which the Grokster and Morpheus software are *capable* of being put, there is evidence to suggest that these are not necessarily popular uses of the software in practice.

The District Court in *Grokster* also held that the defendants did not induce, cause or materially contribute to the infringing conduct. The court held that the defendants' actions in distributing the peer-to-peer filesharing software was not enough to constitute material contribution because the continued existence of the peer-to-peer network was entirely independent of the defendants. As the court pointed out, shutting down Grokster Ltd and StreamCast Networks Inc would have no effect on the operation of their respective networks.

4.1.2 Vicarious infringement

Under US copyright law, a person will be liable for vicarious infringement if that person has: (a) the right and ability to supervise the infringing activity; and (b) a financial interest in that activity.

(a) Napster

The court in *Napster* was satisfied that Napster, Inc had a financial interest in the infringing activities of the users of the Napster networks. Although Napster, Inc had yet to generate any revenue from the Napster software, all the evidence indicated that Napster, Inc planned to cash in on its substantial userbase through one of several proposed revenue generation models.

The court also held that Napster, Inc had both the right and ability to supervise the infringing activity of its users. Napster had, in the past, blocked users from its service for various reasons. Napster argued that it would be technologically difficult to distinguish legal and illegal filesharing on the network. The court rejected this argument.

(b) Grokster

Unlike Napster, Inc, the defendants in *Grokster* had already generated substantial advertising revenues through their software. While these revenues arose from the size of the userbase the networks had attracted, rather than directly from the infringing acts of their users, the court held that the size of the userbase enjoyed by Grokster Ltd and StreamCast Networks Inc had been largely attracted by the availability of infringing works. Accordingly, the court held that the defendants had a financial interest in the infringing activities of the users of their respective networks.

The court held that the defendants in *Grokster* clearly did not have the ability to supervise or control the activities of users of their peer-to-peer filesharing software. The plaintiffs argued (and the defendants disputed) that the defendants could alter their software to give them a degree of

control over users. The court held that, even if true, this was irrelevant to the analysis of vicarious liability. The issue was not whether the defendants could have had the ability to supervise their users if their software had functioned differently, but whether the defendants in fact had the ability to supervise their users using the software as it actually existed.

4.2 Australian copyright law

The only head of indirect liability for copyright infringement in Australia is 'authorisation' of that infringement under section 36 of the Copyright Act 1968. The leading Australian case on authorisation is University of New South Wales v Moorhouse,[21] a case concerning the liability of a university which made a photocopier available to library users for infringing acts committed using that photocopier.

In that case, Gibbs J examined previous decisions which suggested that the failure to actively prevent acts of infringement which one has the ability to prevent may also constitute authorisation, although this would not apply unless the person had knowledge or had reason to suspect that infringement might take place. On the basis of this authority, he gave the following statement of the test for authorisation:

> [A] person who has under his control the means by which an infringement of copyright may be committed – such as a photocopying machine – and who makes it available to other persons, knowing, or having reason to suspect that it is likely to be used for the purpose of committing an infringement, and omitting to take reasonable steps to limit its use to legitimate purposes, would authorise any infringement that resulted from its use.

This interpretation has been criticised as being overly broad and not justified by the wording of the legislation itself. It is certainly much broader that the interpretation of the term in the leading English case on authorisation, *CBS Songs Ltd v Amstrad Consumer Electronics Plc*,[22] in which Templeman LJ held that 'authorisation means a grant or potential grant, which may be express or implied, of the right to do the act complained of'. Nevertheless, *Moorhouse* is now firmly entrenched as the leading Australian authority on the meaning of 'authorisation'.

It is unclear whether defendants such as Grokster Ltd or StreamCast Network Inc would be liable for authorising copyright infringement under Gibbs J's test. Clearly, these parties make the means of infringement available to others, but the other elements are not so clear.

The requirement for the person to have control of the means of infringement begs the question of whether it is necessary for that control to be held at the time of the infringing act. As *Moorhouse* concerned a defendant who did have control of the means of infringement at the time of infringement, the applicability of the *Moorhouse* standard to a case like *Grokster*, where a person relinquishes control over the means of infringement, is unclear. It would be open for an Australian court to follow Gibbs J's formulation of the test in *Moorhouse* but to qualify this first element of the test with a requirement that control be held at the time of the infringement, or perhaps to supplement the test with a *Sony*-style doctrine regarding the liability of a person who relinquishes control over the means of infringement.

It should be noted that any *Sony*-style doctrine in Australia would have a much narrower operation than in the US because, as noted above, Australian copyright law does not feature a doctrine of 'fair use' but rather has the much narrower defence of fair dealing. Accordingly, there will be fewer 'substantial non-infringing uses' for a given technology in Australia than in the US.

The requirement of actual or constructive knowledge is also open to qualification in a case where a person relinquishes control over the means of infringement prior to the infringing act taking place. It would be open to a court to follow *Grokster* and hold that actual knowledge is irrelevant unless it is acquired at a time when the person has the ability to prevent the infringing act and constructive knowledge is subject to a *Sony*-style doctrine.

It is also unclear what the requirement to take reasonable steps to limit the use of the means of infringement to legitimate purposes would require a defendant who relinquishes control over the means of infringement to do in practice. Perhaps a defendant such as Grokster Ltd or StreamCast Networks Inc could argue that the decentralised architecture of next-generation peer-to-peer networks means that there are no reasonable steps that could be taken. Alternatively, the requirement could be interpreted as requiring certain notices or disclaimers to appear on the software.

4.3 Practical considerations

Even if legal action against distributors of next-generation peer-to-peer filesharing software were successful, it would probably be of limited effect as a means of curbing copyright infringement.

While legal action against a creator of next-generation peer-to-peer filesharing software could allow a successful plaintiff to recover damages or an account of profits, the decentralised nature of peer-to-peer networks would still mean that any injunctive relief obtained would be largely futile. As noted by the court in *Grokster*, next-generation peer-to-peer filesharing networks are designed to operate completely independently of their creators and distributors. Even if the distributor ceases to distribute the software, the distribution of modified and improved software amongst the community of users would doubtless continue. Even if no new users began to use the network, the size of the existing FastTrack and Gnutella networks mean these networks could continue to engage in significant levels of copyright infringement for many years.

The problem of identifying, suing and enforcing judgments against creators of peer-to-peer filesharing software are also significant. Sharman Networks, the creator of the KaZaA software, has

distributed different parts of its operation through many holding companies in many countries. As a result, it took the plaintiffs in *Grokster* six months to determine which entity to sue and in which jurisdiction. Other creators of peer-to-peer filesharing software may well follow this example.

5 What other regulatory and technological solutions are available to curb infringement through peer-to-peer networks?

Given that it appears that legal action against users of peer-to-peer networking software is expensive and inefficient and there appears to be no basis (at least under the copyright law as it currently exists) for legal action against creators of peer-to-peer networking software, copyright owners need to explore other ways to curb infringement over peer-to-peer networks.

5.1 Copyright levies

A copyright levy involves the imposition of a levy on the retail sale of recording equipment or blank recording media which Parliament considers is likely to be used by some consumers for the purpose of copyright infringement. Proceeds from the levy are distributed to collecting societies which represent the copyright owners most likely to be affected by the infringement. Copyright levies are currently in place in Germany in relation to CD burners and in the United States in relation to digital recording media.

The major benefit of copyright levies is their effectiveness in lessening the economic costs to copyright owners of copyright infringement because they are practically impossible for purchasers of recording equipment and media to avoid. From an economic point of view, they are a relatively efficient method of redistributing the costs of copyright infringement from copyright owners to copyright infringers. They also attract relatively little consumer backlash because they are generally 'hidden' in the retail price of the product.

However, from a legal point of view, copyright levies are less than satisfactory because they affect all consumers, not just copyright infringers. Effectively, they penalise those who do not infringe copyright and may encourage copyright infringement amongst consumers who consider that they have already paid for the right to infringe copyright. They may either discourage copyright owners from pursuing chronic copyright infringers with legal action or provide copyright owners with a windfall when they succeed against such infringers.

Most critical, however, is the practical problem of how broad such a levy would need to be to cope with large range of equipment and media which consumers may use in the infringement of copyright in relation to digital works. Realistically, such a levy would need to apply to blank CDs and DVDs, CD and DVD burners, all types of memory cards and sticks, hard drives, high capacity floppy disks and disk drives, personal digital assistants, hardware and software MP3 players and Internet based data storage services – as well as any other recording equipment and media which comes into existence in the future. To apply to only a subset of this media would be to unfairly favour one recording media over another. Yet to apply a levy to all these media would make the levy even less attractive from a legal perspective as it reduces the percentage of likely copyright infringers as a proportion of all consumers of these products.

5.2 Disruptive powers for copyright owners

Some members of the US Congress have indicated support for the idea of allowing copyright owners to take direct technological action against copyright infringers.

A range of measures has been proposed, including allowing copyright owners to 'destroy [an infringer's] computer';[23] permitting copyright owners to hack into networks to detect infringing activity; permitting copyright owners to prevent others downloading their copyright works by monopolising the bandwidth of any node which is hosting infringing copies of those works; permitting copyright owners to place fake versions of their copyrighted works on networks; and permitting copyright owners to distribute viruses through networks.

These methods may be effective in practice to curb copyright infringement, but they are unappealing from a legal perspective because they all involve acts which are potentially prohibited under computer crime, consumer protection and other laws. It would be highly inappropriate for the law be seen to encourage or condone such vigilante behaviour. To do so would likely affect many innocent users of peer-to-peer filesharing software and encourage further malicious conduct by both copyright owners and copyright infringers. This was illustrated by the recent retaliatory defacement of Madonna's web site after the popular singer released fake versions of her new album on the FastTrack network.[24]

5.3 Technological measures – Digital rights management and encryption

The technological measure of 'digital fingerprinting' – identifying copyrighted works by recognising data patterns – was used to identify infringing works on Napster but appears to be of limited assistance in curbing infringement in next-generation peer-to-peer filesharing networks, because the decentralised nature of these networks mean that there is no central point at which a digital fingerprinting filter can be applied.

Two other related technological options for curbing copyright infringement appear more promising. The first is digital rights management, which involves building access and use restrictions into a digital work – for example, a restriction which permits a song to be played only a certain number of times or which prevents a song from being burnt to a CD. The leading consortium engaged in developing digital rights management

for audio content is the Secure Digital Management Initiative ('**SDMI**'). SDMI rights management is centred around the use of digital watermarks – an identification code which is 'hidden' in an audio file and which provides information about the origin and authenticity of the file. SDMI digital watermarks restrict the subsequent use of an audio file which has been compressed – for example, into MP3 format.

The second technological measure is encryption. The encryption of media files means that only authorised hardware and software have the key to allow them to decrypt and play that media. An example is the Content Scrambling System, the encryption which protects DVD movies.

The key benefit of digital rights management and encryption is that they are relatively simple technological measures, and any attempt to circumvent SDMI or to distribute a device which circumvents SDMI is likely to be prohibited by the US *Digital Millennium Copyright Act* (the '**DMCA**') and the Digital Agenda amendments to the Australian *Copyright Act*.[25] This legislation makes it an offence to circumvent, or to distribute a device capable of circumventing or facilitating the circumvention of, a measure designed to prevent or inhibit the infringement of copyright in a work. *Universal City Studios v Reimerdes*[26] involved successful application of the DMCA to injunct the defendants from distributing the distribution of DeCSS, software designed to circumvent CSS encryption.

There are two main disadvantages of digital rights management and encryption.

Firstly, technological protection measures such as digital rights management and encryption have in the past proven relatively easy for hackers to circumvent. In 2001, SDMI invited hackers to try to defeat their digital watermark technology in a public contest. Despite several hacker groups boycotting the contest, all proposed watermark technologies were swiftly defeated by multiple contestants. CSS was circumvented by a 15 year old student from Norway, chiefly because the encryption master key was inadequately secured by a single software developer. It is evident that significant advances in encryption methods must be made before encryption can become a viable method of protecting copyrighted works.

Secondly, measures such as digital rights management and encryption both threaten to extend copyright beyond the traditional bundle of rights afforded to copyright owners under copyright law and intrude on the 'fair use' and 'fair dealing' exceptions to copyright.

US fair use and Australian fair dealing exceptions permit the doing of certain acts for certain purposes which would otherwise constitute infringement of copyright. Digital rights management technologies can prevent consumers from engaging in these sorts of fair uses and fair dealings by making it technologically difficult to copy copyrighted works in whole or in part. Because the technology cannot readily distinguish between a fair use or a fair dealing and an infringement, the technology errs in favour of preventing legitimate fair uses and fair dealings.

To swing the balance even further against fair use and fair dealing, the DMCA and the Australian *Copyright Act* each prohibit the circumvention of a technological protection measure, even if that circumvention is intended solely to enable a fair use or fair dealing to be made. So even if the technology can be defeated, it remains illegal to do so to engage in an otherwise legitimate use.

It seems unlikely that technological protection measures could ever be properly adapted to permit all fair uses or fair dealings by consumers and yet remain effective to prevent copyright infringement. Even in the narrower, Australian concept of fair dealing, it is impossible to specify whether copying a particular number of pages or number of seconds of a work will amount to a fair dealing, without a full knowledge of the context in which the copying occurred. The problem is even greater in relation to the US concept of fair use, which is designed to evolve as new technological problems arise.

6 Conclusion

After *Napster*, many assumed that copyright infringement over peer-to-peer filesharing software could be readily curbed by legal action against distributors of peer-to-peer filesharing software and a few high-volume users. After *Grokster*, it now appears that distributors of next-generation peer-to-peer filesharing software cannot be held liable for the actions of their users under existing copyright law. Even if the legislature intervenes to change the existing copyright law, such legal actions are still unlikely to affect the existence and growth of peer-to-peer filesharing networks. The route the RIAA is currently pursuing, that of legal action against the large number of users engaged in copyright infringement, appears to be an expensive and ultimately futile exercise.

Accordingly, it appears that copyright owners will need to look towards other regulatory and technological solutions to curb copyright infringement over peer-to-peer filesharing software. The most promising of these appears to be technological protection measures, such as digital rights management and encryption. However, there are significant technical and legal obstacles to be overcome before these measures can be widely adopted – they have in the past proved vulnerable to hackers and have a tendency to curtail non-infringing, as well as infringing, uses.

While past technological advances such as the VCR were greeted by a great deal of scaremongering by copyright owners which ultimately proved unfounded, the advent of next-generation peer-to-peer filesharing software appears to put copyright owners in a genuinely difficult situation when it comes to protecting their rights. It will be very interesting to see how both the law and the technology develops as copyright owners seek to find a solution to the problem of copyright infringement over next-generation peer-to-peer filesharing networks.

1 'MP3' is a popular format which allows music recorded in compact disc format to be compressed into manageable file sizes with little loss of quality: *Napster* 114 F Supp 2d 896, 901 [A] (ND Cal 2000).

2 *A&M Records Inc v Napster, Inc* 114 F Supp 2d 896 (ND Cal 2000) ('*Napster*').

3 *A&M Records Inc v Napster, Inc* 239 F 3d 1004 (9th Cir 2001).

4 Stephanie Green, 'Reconciling Napster with the Sony decision and recent amendments to copyright law' (2001) 39 *American Business Law Journal* 57, 98.

5 *Metro-Goldwyn-Mayer Studios Inc v Grokster Ltd* Nos CV-01-08541-SVW, CV-01-09923-SVW (CD Cal, 25 April 2003) ('*Grokster*') (available at www.cacd.uscourts.gov).

6 *Grokster* Nos CV-01-08541-SVW, CV-01-09923-SVW (CD Cal, 25 April 2003), 21-2.

7 *Copyright Act of 1976* 17 USC s 106.

8 *Napster* 114 F Supp 2d 896, 911 [B2] (ND Cal 2000); *A&M Records Inc v Napster, Inc* 239 F 3d 1004, 1014 (9th Cir 2001).

9 *Grokster* Nos CV-01-08541-SVW, CV-01-09923-SVW (CD Cal, 25 April 2003), 8-10.

10 *Copyright Act 1968* (Cth) ss 31(1)(a)(i), 31(1)(b)(i).

11 *S W Hart & Co Pty Ltd v Edwards Hot Water Systems* (1985) 159 CLR 466; *CCOM Pty Ltd v Jiejing Pty Ltd (No 2)* (1993) 48 FCR 41.

12 *Autodesk Inc v Dyason* (1992) 173 CLR 330.

13 *Copyright Act 1968* (Cth) ss 85(1)(a), 86(a), 101(1), 101(3).

14 *Copyright Act 1968* (Cth) s 10(1).

15 *Copyright Act 1968* (Cth) s 10(3)(c).

16 *Copyright Act 1968* (Cth) ss 31(1)(a)(iv), 31(1)(b)(iii), 85(1)(c), 86(c).

17 *Copyright Act 1968* (Cth) s 10(1).

18 Recording Industry Association of America, 'Recording Industry To Begin Collecting Evidence and Preparing Lawsuits Against File 'Sharers' Who Illegally Offer Music Online' (25 June 2003) <http://www.riaa.com/news/newsletter/062503.asp>

19 *A&M Records Inc v Napster, Inc* 239 F 3d 1004 (9th Cir 2001).

20 *Sony Corporation of America v Universal City Studios Inc* 464 US 417, 442 (1984) ('*Sony*').

21 (1975) 133 CLR 1 ('*Moorhouse*').

22 [1988] RPC 567 (HL).

23 'Hatch wants to fry traders' PCs', *Wired News* (18 June 2003) http://www.wired.com/news/digwood/0,1412,59298,00.html.

24 Ashlee Vance, 'Like a virgin - Madonna hacked for the very first time' The Register (22 April 2003) <http://www.theregister.co.uk/content/6/30356.html>

25 *Copyright (Digital Agenda) Amendment Act 2000* (Cth) amending the *Copyright Act 1968* (Cth)

26 *Universal City Studios, Inc v Reimerdes* 111 F Supp 2d 294 (SDNY 2000).