Kazaa goes the way of Grokster? Authorisation of copyright infringement via peer-to-peer networks in Australia

Rebecca Giblin-Chen and Mark Davison*

In Universal Music Australia v Sharman License Holdings (2005) 65 IPR 289 an Australian Federal Court suggested for the first time that it is acceptable to prohibit the continued distribution of a product on the grounds that after its sale it is capable of being used by its purchaser to infringe copyright, even though it may also have non-infringing uses. The decision, currently on appeal to the Full Court, raises important questions about the scope and meaning of the concept of "authorisation" under Australian law. The most important question is whether or not some degree or control is necessary to support a finding of authorisation. This article comprehensively explains the decision and argues that the Full Court could usefully draw upon some aspects of the United States approach to answer the questions raised.

Kazaa[1] is a controversial peer-to-peer file sharing system that has helped build an empire on copyright infringement. First released in July 2000,[2] by early 2004 it had been downloaded more than 317 million times.[3] It facilitates the transfer of billions of files each month, most of which are infringing.[4] But it has been stopped in its tracks by a decision of the Australian Federal Court in *Universal Music Australia v Sharman License Holdings* (2005) 65 IPR 289 in which Justice Murray Wilcox held that several companies and individuals behind the notorious software can be held liable for the copyright infringements of its users.[5] While pecuniary damages will be assessed at a subsequent hearing,[6] Wilcox J issued an injunction that seems likely to finally end the Kazaa free-for-all.

Two aspects of this decision are particularly noteworthy. First, the court's analysis raises pertinent questions about the scope and meaning of the concept of "authorisation" under Australian law. Second, the framing of the injunction suggests, for the first time in a common law country, that it is acceptable to prohibit the continued distribution of a product on the grounds that after its sale it is capable of being used by its purchaser to infringe copyright, even though it may also have non-infringing uses.

* Rebecca Giblin-Chen, PhD student, Faculty of Law, Monash University. Mark Davison, Professor, Faculty of Law, Monash University. The authors wish to acknowledge the pictorial demonstration of the Kazaa system contributed by Mr JC Chen.

[1] Once capitalised as KaZaA, but now generally referred to simply as Kazaa.

[2] Borland J and Mariano G, *Looking for the next Napster* http://news.com.com/Looking+for+the+next+Napster/2009-1023_3-269454.html viewed 18 May 2005.

[3] "At the beginning of 2004, the Kazaa website was claiming that over 2.4 million people downloaded the Kazaa software during the previous week; that is, there were over 2.4 million new users that week. The KMD webpage claimed total downloads of 317,552,315 people. That figure equates to about 5% of the world's human population": *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 337.

[4] Altnet, one of the respondents held liable for authorisation of copyright infringement, claimed that Kazaa's 60 million users downloaded over three billion files each month. *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 329. Wilcox J noted that while it was theoretically possible for the system to be used to transfer non-infringing files, "in May 2003, Kazaa was being predominantly used for music file-sharing. A reader who had even a general understanding of copyright law would also have realised this necessarily involved copyright infringement on a massive scale": *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 337. Accordingly it is appropriate to surmise that the number of unauthorised transfers of copyrighted material each month amounted to billions.

[5] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 399.

[6] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 299.

This article provides the reader with an insight into several vital issues.

Part 1 uncovers Kazaa's technological and corporate secrets. It examines the complex corporate structure adopted by the defendants and the factors leading to the liability of some but not all of the respondents for the authorisation of copyright infringement. It then goes on to give a detailed explanation of the technology employed by the defendants. This explanation is critical to understanding the relationship between that technology, the findings of liability against most of the defendants and the nature of the injunctive relief granted by Wilcox J.

Part 2 details the decision in relation to each of the respondents. It then explains the injunction and the technological and practical implications of satisfying its requirements.

Part 3 explains how the decision augments and, arguably, fundamentally changes the law relating to the concept of authorisation under Australian copyright law. In particular, it argues that at least one aspect of the injunction goes beyond anything ever done in copyright law and is possibly contrary to existing authority on the point.

Part 4 highlights the similarities and differences between the Australian concept of authorisation and the United States concept of secondary liability for copyright infringement, with particular reference to the recent decision of the United States Supreme Court in *MGM Studios Inc v Grokster Ltd* 125 S Ct 2764 (2005). It argues that the Australian law may usefully draw upon the United States approach in answering some of the questions that this decision raises.

If upheld on appeal this decision is likely to cripple Kazaa. However, the development and distribution of peer-to-peer software by others will continue. Consequently, the focus of this article is predominantly on the implications of this decision for copyright owners and software developers in Australia.

PART 1. UNLOCKING KAZAA'S SECRETS

A. Through the looking glass: A complex corporate structure

Kazaa was born when entrepreneurial businessmen Niklas Zennström and Janus Friis quit their jobs at a Swedish internet service provider in the late 1990s, determined to make their fortunes.[7] Napster was already creating a maelstrom within the recording industry. After tossing up several ideas, they decided that they, too, should create a peer-to-peer file sharing program. Though neither knew how to write computer programs, that was no deterrent. They simply took their idea to a team of Estonian programmers and asked them to bring it to fruition.[8] Zennström and Friis owned the resulting software through Dutch company Kazaa BV.[9]

Kazaa actually encompasses two separate pieces of software. The first is Kazaa Media Desktop (KMD). KMD is client software. A client is a special type of computer program that can request services (usually over the internet) from other programs.[10] KMD is used to facilitate searches and transfers of files over the internet.

The second piece of software is called "FastTrack". FastTrack is a protocol. A protocol is the set of rules that governs communications between devices, such as computers on a network.[11] The FastTrack protocol dictates how the network operates, including how searches are performed, how users connect to each other and so on. Essentially, KMD is pre-programmed to obey FastTrack's rules. Collectively, KMD and FastTrack are referred to within this article as "Kazaa", although at times the distinction between the two is critical and will be reiterated.

[7] Roth D, "Catch Us If You Can" (2004) 149(2) *Fortune.*
[8] Roth, n 7.
[9] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 318.
[10] *Client* http://dictionary.oed.com.ezproxy.lib.monash.edu.au/cgi/entry/50041458?single=1&query_type=word&queryword=client&first=1&max_to_show=10 viewed 17 August 2005.
[11] *Protocol* http://dictionary.oed.com.ezproxy.lib.monash.edu.au/cgi/entry/50190799?query_type=word&queryword=protocol&first=1&max_to_show=10&sort_type=alpha&result_place=1&search_id=6UUH-A3oPJX-14375&hilite=50190799 viewed 14 April 2005.

KMD has been licensed to several other companies. The licences give those companies the rights to distribute their own branded versions of KMD, but do not convey the right or ability to make alterations to the software. The Grokster technology that was at issue in the recent United States Supreme Court decision is itself an independently "branded, marketed and distributed" version of KMD.[12] As all versions of KMD follow FastTrack's rules regardless of their branding, the users of each connect to what is called the "FastTrack network". An individual using the Grokster software can share files seamlessly with an individual using KMD.

Kazaa quickly drew the attention of content interests, which instituted litigation against it in both the Netherlands and the United States. The Dutch case was decided first. In November 2001 the Amsterdam District Court granted the application of the Dutch copyright association for an injunction against Kazaa BV, and ordered Kazaa to be shut down within 14 days.[13]

Kazaa BV responded quickly. Within weeks of the Dutch decision, businessman Kevin Bermeister had told associate Nicola Hemming that Kazaa BV was looking to sell its assets.[14] Ownership of the FastTrack technology was transferred to Joltid Ltd[15] (Joltid), a Virgin Islands company owned by Zennström.[16] Then there was a flurry of incorporations. In January, Sharman Networks (Sharman) was incorporated in Vanuatu. Sharman Holdings followed suit in June.[17] In February LEF Interactive was incorporated in Australia, with Ms Hemming its sole director and shareholder.[18]

With this structure in place, Sharman entered into agreements with Kazaa BV to purchase its peer-to-peer business and an irrevocable licence to software including KMD.[19] It also entered into an agreement with Joltid for a broad-ranging and irrevocable licence to FastTrack.[20] These licences included the right and ability to make alterations to the Kazaa software.

Also in February 2002 a company called Altnet was incorporated in the United States under the sole directorship of Mr Bermeister.[21] It was jointly owned by Brilliant Digital Entertainment, of which Mr Bermeister was President and CEO, and Joltid.[22] In 2003, Altnet and Sharman formally entered into a joint venture agreement under which Altnet obtained the exclusive right to provide responses to search requests initiated by Kazaa users. These responses would be for authorised copies of music that could be downloaded by users on a commercial basis.[23]

In March 2002 the Amsterdam Court of Appeal overturned the District Court's decision to grant an injunction against Kazaa BV,[24] a decision eventually upheld by the Dutch Supreme Court.[25] This suggests that these complex arrangements may have been too hasty. Nonetheless, they still served to obscure Kazaa's true ownership and delay legal action by content interests. Indeed, Kazaa's ownership still remains a mystery despite the best efforts of the applicants. Under Vanuatu law, it is an offence to reveal the controllers behind any Vanuatu international company.[26] The court

[12] *MGM Studios Inc v Grokster Ltd* 243 F Supp 2d 1073 at 1080 (CD Cal, 2003).
[13] *Vereniging Buma and Stichting Stemra v Kazaa BV* (unreported, Amsterdam District Court, 29 November 2001).
[14] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 318.
[15] Formerly known as "Blastoise Ltd". *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 319.
[16] *MGM Studios Inc v Grokster Ltd* 243 F Supp 2d 1073 at 1081 (CD Cal, 2003).
[17] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 317.
[18] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 319.
[19] Note that the licence was non-terminable except under clause 6 of the agreement. *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 319.
[20] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 319.
[21] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 320.
[22] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 320.
[23] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 321.
[24] *Kazaa BV v Vereniging Buma and Stichting Stemra* No 1370/01 (Unreported, Amsterdam Court of Appeal, 28 March 2002).
[25] *Vereniging Buma and Stichting Stemra v Kazaa BV* C02/186HR (Unreported, Supreme Court of the Netherlands, 19 December 2003).
[26] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 317.

discovered that both Sharman companies were controlled by two Vanuatu accountants, probably acting on behalf of others.[27] But the identities of the ultimate owners remain unknown.[28]

B. Inside the technology

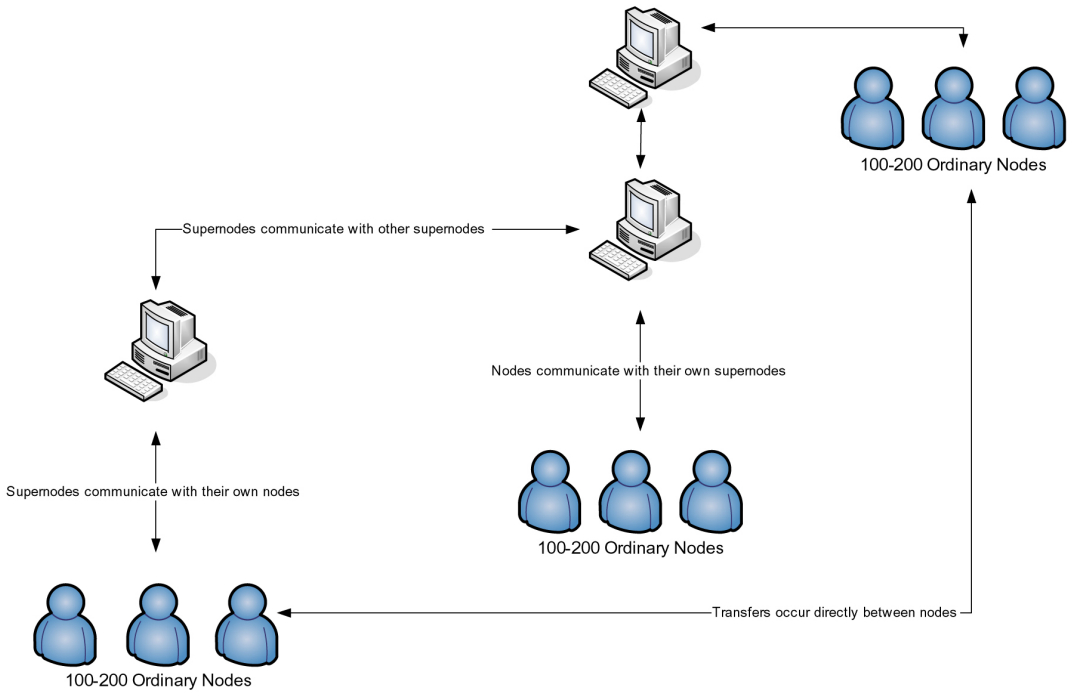
There are several ways to determine how a software program works. The first and by far the most effective way is to examine the program's source code. When a programmer initially writes a program he or she writes it in source code. This is the only type of code that is easily comprehensible to humans. In order to execute the program, however, it must be translated into a language that a computer can understand, or machine code. In some cases the programmer will make the source code openly available so that others can understand how it works. This is known as "open source". In Kazaa's case however, the source code is closed.[29] In fact, Kazaa's source code is kept so secret that Wilcox J was not even entirely convinced that the true source code was provided at the trial.[30]

Without access to the source code it may be possible to ascertain much of what the software does through observation. However, much detail will be lost because of an inability to determine *how* it does it. This has meant that despite Kazaa's incredible saturation level, prior to this trial little was known about how it actually works. In his lengthy judgment Wilcox J undertook a painstaking exploration of the technology and its relationship with the law, which added significantly to the available knowledge of the Kazaa system. The judgment indicates a thorough command of the technical aspects of the software in very difficult circumstances. Despite evidentiary problems at the trial, the decision authoritatively and comprehensively clarifies how the Kazaa system operates.

Unlike the early peer-to-peer file sharing program Napster, Kazaa probably does not have a central server.[31] In the absence of a server, all communications necessary to run the network obviously must be transmitted between the users themselves. This fact caused an early version of another decentralised peer-to-peer network to run into trouble when users with obsolete computer equipment and slow dial-up connections caused the network to bottleneck.[32] The FastTrack protocol gets around this difficulty by taking advantage of the heterogeneity of its users. Those users with powerful computers and lightning broadband internet connections are automatically required to carry a heavier load of network traffic, while the slower ones are required to do much less. This creates a "two-tiered organisational structure" consisting of supernodes (the fast users) and ordinary network nodes (the slow users).[33]

This structure is demonstrated pictorially below.

[27] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 317-318.
[28] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 317-318.
[29] *MGM Studios Inc v Grokster Ltd* 259 F Supp 2d 1029 at 1032 (CD Cal, 2003).
[30] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 339.
[31] The issue of whether the Kazaa system does in fact have a central server was very contentious and the subject of much argument and evidence during the course of the trial. However, on the evidence Wilcox J was unable to find that that the Kazaa system had a central server at this time. *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 345.
[32] Truelove K, *Gnutella: Alive, Well, and Changing Fast* http://www.openp2p.com/lpt/a/573 viewed 4 May 2005.
[33] *MGM Studios Inc v Grokster Ltd* 259 F Supp 2d 1029 at 1040 (CD Cal, 2003).



Each time a user connects to the FastTrack network through the KMD software he or she is designated either a node or a supernode. This allocation of status occurs automatically and is dependent on demand. Accordingly, a user who was a supernode the previous time he or she connected may be an ordinary node the next. Once a user becomes a supernode, KMD automatically sends messages to other supernodes announcing its presence. Soon afterwards, geographically proximate ordinary nodes will begin to connect. It appears that between one hundred and two hundred ordinary nodes generally connect to each supernode.[34] Every user who is not currently a supernode is an ordinary node.

Every time KMD is installed, a shared folder is created on the new user's computer.[35] The default setting provides that the contents of this shared folder are accessible to other network users. Once each minute the supernodes scan the shared folders of each of the ordinary users to which they are connected and compile an up-to-date index of all available files.[36] The index contains several pieces of information. First, it contains "metadata" about each file. Metadata is a term that simply describes data about other data.[37] If the particular file is a song, the metadata often includes the song title, artist name, file description and file size.[38] The index also contains a filehash. A filehash is a unique sequence of digits that identifies that file.[39] Every identical copy of a file will have an identical filehash, but even minor changes will result in the file receiving an entirely different filehash. Finally,

[34] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 309.
[35] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 309.
[36] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 309.
[37] *Metadata* http://dictionary.oed.com.ezproxy.lib.monash.edu.au/cgi/entry/00307096/00307096se19?single=1&query_type=word&queryword=metadata&first=1&max_to_show=10&hilite=00307096se19 viewed 8 September 2005.
[38] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 309.
[39] For more information about filehashes and how they are determined for each file, see *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 309.

the index lists the location of each of the files.[40] Internet locations are designated with unique internet protocol addresses (IP addresses) which allow machines on networks to be distinguished from each other and to be located by others.[41]

When an ordinary node performs a search in KMD two things occur. First, an encrypted message is sent to the supernode. The supernode automatically decrypts the message and checks the search terms against its continually-updating index. Then the supernode automatically encrypts the search results and sends them back to the requesting node. If there were few or no results, the supernode will re-encrypt the search request and send it to the other supernodes it is connected to, which will in turn decrypt it and check the search terms against their own indexes and send their responses via the originating supernode. All of the files that are discovered by a search within this ordinary node/supernode relationship are known as "blue" files.[42]

Each search result contains the IP address of the user who has the desired file. The requesting user can download a blue file by simply clicking the "download" icon next to the relevant search result. Clicking on the link sends a request for the relevant filehash to the supplying user, and if that user is still online (and not prevented from sending files by any technical limitations) a direct link will be established to transmit the file.[43] The file is automatically saved in the shared folder of the receiving user and made available to other network users.

The second thing that occurs when an ordinary node performs a search in KMD is that the search request is sent to the "TopSearch" index in the user's own computer. The TopSearch index is maintained by Altnet and contains files known as "gold' files (as distinct from the "blue" files supplied by individual users). The provision of gold files is authorised by their respective copyright owners. The TopSearch index contains information such as song titles and artist names. As well as containing information that is specifically relevant to the actual file, it may also tie the gold file to unrelated keywords. For example, the gold file owner of a particular Christina Aguilera song may think that Madonna fans would be interested in it. By linking with the keyword "Madonna" they could ensure that any search for "Madonna" would receive a result for the Christina Aguilera file. Updated copies of the index are regularly sent to all online Kazaa users by Altnet computers.[44] Should a user wish to download a gold file, he or she may be required to enter into a licence agreement and pay a fee (although many gold files are available on a free trial basis). Gold files contain protections against unauthorised copying and cannot be distributed on the FastTrack network without the facilitation of Altnet. Altnet claims to have the ability to respond to 120 million Kazaa search requests per day.[45]

In Kazaa's current format, each search request can only return a maximum of 200 results. This maximum limit applies regardless of how many of the results are blue and how many are gold.[46]

One final relevant feature of Kazaa is the "participation level". Participation levels are determined "by the ratio of the amount of data downloaded by an individual Kazaa user as opposed to the amount uploaded from that user's computer".[47] Users with higher participation levels are rewarded with increased network priority, which often makes it easier for them to download other files.[48]

[40] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 309.
[41] IP addresses are commonly expressed as four octets (4 lots of 8 bits) separated by full stops. An IP address will look something like 64.78.205.207.
[42] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 310.
[43] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 310.
[44] This is problematic. The court has not explained how Altnet is able to send its updated index to all online Kazaa users if there is no central server to identify the internet locations of those online users. For more information about how TopSearch works, see *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 325.
[45] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 325.
[46] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 364.
[47] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 311.
[48] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 311.

PART 2. AUTHORISATION UNDER AUSTRALIAN LAW

The trial was divided into two parts, with pecuniary remedies to be considered at a later date.[49] This decision relates to the liability issues and non-pecuniary remedies.

The applicants made several claims. The main one was that the respondents were liable for copyright infringement under the *Copyright Act 1968* (Cth) for authorising Kazaa's users to themselves commit copyright infringement. Wilcox J upheld this claim as against several of the respondents. Wilcox J's findings of infringement of copyright and authorisation are explained at A. The injunctive relief granted to the applicants against those found to have authorised copyright infringement is explained at B. Part 3 follows with a more detailed analysis of the concept of authorisation under Australian law, the reasons for those findings and their relationship to that injunctive relief.

Several peripheral claims were also raised in this litigation. It was alleged that the respondents engaged in misleading conduct and unconscionable conduct in violation of the *Trade Practices Act 1974* (Cth) and the *Fair Trading Act 1987* (NSW) as well as conspiracy to injure and conspiracy by unlawful claims. These claims were dismissed and will not be dealt with further in this article**.**

A. The authorisation analysis

The *Copyright Act 1968* (Cth) (the Act) provides that copyright will be infringed where a person who is not the owner or licensee authorises the doing in Australia of any act comprised in the copyright.[50] Thus, it requires a two-step analysis:

1. A person must infringe or threaten to infringe the copyrighted work; and
2. That infringement or threatened infringement must have actually been authorised by the defendant when he or she was not authorised to do so.

While Kazaa has probably been used to facilitate billions of copyright infringements,[51] in order to precisely identify the primary infringement for the purposes of this litigation the applicants confined their claim to the authorisation of infringement of 98 identified sound recordings.[52] It was mutually accepted that these identified sound recordings fell within the statutory definition of "sound recording" and that copyright subsisted in them.[53]

Any user who connects to the FastTrack network with copies of copyrighted material in their shared folder makes the copies available online and thereby infringes the right of communicating to the public.[54]

No evidence was led to identify any particular Kazaa user who made available any of the 98 identified sound recordings.[55] However, there was uncontested evidence that each of the recordings was available for download as a "blue" file on the FastTrack network.[56] Accordingly, the court held that this was sufficient evidence of infringement.

The court held that several but not all of the respondents had authorised the infringement of the identified sound recordings pursuant to s 101(1) of the Act. The application of the law to each of the respondents is outlined below.

Sharman Holdings and Sharman Networks

Insufficient evidence was led regarding Sharman Holdings Pty Ltd to support a finding of authorisation of infringement.[57] However for Sharman Networks the situation was different.

[49] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 299.
[50] *Copyright Act 1968* (Cth) s 101(1).
[51] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 332.
[52] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 299.
[53] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 375.
[54] *Copyright Act 1968* (Cth) s 85(1)(c).
[55] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 387.
[56] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 387.
[57] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 385.

By virtue of s 112E, which is fully explained in Part 3,[58] Sharman would not be liable for authorisation merely because it provided the facilities that facilitated users' infringement.[59] Something more would be needed.

However, Sharman's provision of facilities *was* relevant to the nature of the relationship existing between Sharman and the infringing Kazaa users.[60] If Sharman had not provided those facilities, the infringing users would not have been able to use the Kazaa system to infringe.

Other factors were also suggestive of authorisation. Sharman was described by the court as "the operator of the Kazaa system".[61] It also noted that "it has been in Sharman's financial interest for there to be ever-increasing file-sharing, involving an ever-greater number of people"[62] and that "Sharman always knew users were likely to share files that were subject to copyright".[63] Even if this had not always been known, there was conclusive evidence that it had been known since at least May 2003. At that time market research company Syzygy Branding supplied Sharman Networks with a report which made it clear that most Kazaa users were using it to download unauthorised copies of music. The report also suggested that any move away from this model would be likely to lose users.[64] Any loss of users would have a negative effect on revenue.

There was also evidence that Sharman had engaged in positive acts that encouraged copyright infringement. Given that Sharman knew that Kazaa users were actually using Kazaa to infringe, these factors are particularly damning.[65] They included:

1. Website promotion of KMD as a file-sharing facility;[66]
2. "Exhortations" to users to use KMD and share their files;[67] and
3. Promotion of the "Join the Revolution" movement, which is "based on file-sharing, especially of music, and which scorns the attitude of record and movie companies in relation to their copyright works".[68]

Another positive act was to design the software in such a way that it encouraged the uploading of files through the use of participation levels. As described above, participation levels are determined "by the ratio of the amount of data downloaded by an individual Kazaa user as opposed to the amount uploaded from that user's computer".[69] Users with higher participation levels are rewarded with increased network priority, making it easier for them to download other files.[70] This feature encourages individuals to upload more material. The predominant material on the network was known by Sharman to be popular music, all or almost all of which was unauthorised.[71] If users made popular music available from their computers in breach of copyright, it would be likely to be downloaded by others and have a positive effect on their participation level. However, if they only made authorised material available, for which there was much less demand, it would be likely to have

[58] Section 112E provides that a person (including a carrier or carriage service provider) who provides facilities for making, or facilitating the making of, a communication is not taken to have authorised any infringement of copyright in an audio-visual item merely because another person uses the facilities so provided to do something the right to do which is included in the copyright.
[59] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 385.
[60] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 385.
[61] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 385.
[62] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 385.
[63] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 385.
[64] See *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 329-330.
[65] See *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 386.
[66] See *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 312-314.
[67] See *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 312-314.
[68] See *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 314-315 and 335-336. The court also noted that "Especially to a young audience, the 'Join the Revolution' website material would have conveyed the idea that it was 'cool' to defy the record companies and their stuffy reliance on their copyrights": *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 386.
[69] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 311.
[70] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 311.
[71] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 337.

little or no effect on their participation level. Accordingly, the existence of this feature suggests that Sharman was encouraging its users to make popular material available in breach of copyright.

Controversially, the Act requires the court to take into account the extent of Sharman's power to prevent the infringement.[72] The respondents argued that there could be no finding of authorisation unless Sharman was able to "control" the behaviour of Kazaa users.[73] Without finally deciding this question however, the court held that Sharman "was in a position, through keyword filtering or gold file flood filtering, to prevent or restrict users' access to identified copyright works; in that sense, Sharman could control users' copyright infringing activities".[74] The proposed keyword filtering and gold file flood filtering measures are explained at B.

The court was also required to take into account the steps Sharman took to prevent or avoid the Kazaa users' infringements.[75] The court could find only two such steps. First, the promotional statements made on the Kazaa website each bore a notice (in small print) that Sharman does not "condone activities and actions that breach the rights of copyright owners".[76] Second, the End User License Agreement (EULA) that each user was required to agree to in order to install KMD stated that the program was not to be used for copyright infringement.[77] However, the court seemed to consider these to be token efforts:

> It is difficult to believe those directing the affairs of Sharman, or any of the other respondents, ever thought these measures would be effective to prevent, or even substantially to curtail, copyright file-sharing. It would have been obvious to them that were those measures to prove effective, they would greatly reduce Kazaa's attractiveness to users and, therefore, its advertising revenue potential. However, if any of those people did have such a view, it could not have survived receipt of the Syzygy report.

Having regard to the available evidence, the court held that Sharman infringed the applicants' copyright in their 98 identified recordings "by authorising Kazaa users to make copies of those sound recordings and to communicate those recordings to the public".[78] Furthermore, the continued existence of Kazaa in its current form would threaten to infringe other copyrights.[79]

LEF Interactive and Ms Hemming

Having decided that Sharman was liable, the court went on to consider whether Ms Hemming and LEF Interactive should be held liable for Sharman's infringement.[80] Ms Hemming was LEF Interactive's sole director and shareholder, and the court held that it was in fact Ms Hemming's alter ego.[81] Accordingly, it was held that "no distinction should be made between the position [sic] of these two respondents".[82]

Wilcox J went on to review the circumstances in which it is appropriate to hold a director of a corporation personally liable for its torts. There are three possible tests. The "Performing Right Society test" provides that "a director is personally liable for a tortious act committed by the company which the director has ordered or procured to be done".[83] This has been criticised for being too broad. Stricter is the "Mentmore test", which holds liable a director or officer who makes "the tortious act his own".[84] However, this test has been criticised for being unclear as to what conduct would be sufficient to satisfy it.[85] The third test was suggested by Finkelstein J in *Root Quality Pty Ltd v Root*

[72] *Copyright Act 1968* (Cth) s 101(1A)(a).
[73] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 387.
[74] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 387.
[75] *Copyright Act 1968* (Cth) s 101(1A)(c).
[76] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 386.
[77] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 316-317.
[78] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 388.
[79] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 388
[80] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 388.
[81] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 388.
[82] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 388.
[83] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 389.
[84] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 389.
[85] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 389-390.

Control Technologies Pty Ltd (2000) 177 ALR 231; 49 IPR 225; [2000] FCA 980. It provides that a director can be held personally liable where his conduct is such "that it can be said of him that he was so personally involved in the commission of the unlawful act that it is just that he should be rendered liable".[86] The court adopted this test.[87]

While up to 19 individuals at a time had worked for LEF Interactive, and there existed a Sharman executive committee that met to discuss "issues",[88] the court found that Ms Hemming was undeniably in charge:

> Ms Hemming is "the boss" … Whatever the ultimate ownership of the company, Ms Hemming has always been in charge of its day-to-day activities. There is no reason to doubt that she formulates, or at least approves, Sharman's policies.[89]

Ms Hemming was also aware of the fact that KMD was largely used for copyright infringement – from the date of the Syzygy report if not before.[90] However, despite being in a position of responsibility and control, she did not appear to have done anything to eliminate or reduce the infringement.[91]

Accordingly it was held that LEF Interactive and Ms Hemming had also authorised the Kazaa users' infringements.[92]

Mr Morle

The court went on to consider whether Mr Morle should be held liable for Sharman's infringements. Mr Morle was employed by LEF Interactive as Sharman's "Director of Technology".

The court engaged in the same analysis as for Ms Hemming, but came to the opposite conclusion. Unlike Ms Hemming, Mr Morle was a "mere employee" and had no financial interest in Sharman:

> [T]he evidence fails to demonstrate that Mr Morle was in such a dominant position in Sharman that he can be said even to have procured and directed those acts and omissions, still less that he can be said to have made those acts his own or to have acted deliberately or maliciously to infringe the applicants' rights.[93]

Accordingly, Mr Morle was not liable for authorisation of copyright infringement.

Altnet, Brilliant Digital Entertainment and BDE Pty Ltd

BDE Pty Ltd is an Australian company that appears to be linked to Brilliant Digital Entertainment and Altnet. The court noted that insufficient evidence was led regarding BDE Pty Ltd's activities for it to be held liable for Sharman's authorisation.[94]

The applicants alleged that the Altnet and Brilliant Digital Entertainment (the Altnet companies) should also be held liable for Sharman's authorisation of infringement because their business was "extremely closely aligned if not inextricably linked" to Sharman.[95] Altnet is the company that provides the gold files to Kazaa's users; Brilliant Digital Entertainment is its part-owner. As the Altnet companies were so closely linked the court held any liability of one must be shared by the other.[96]

Altnet argued that it should not bear any responsibility for authorisation of infringement because it was only responsible for providing gold files to the Kazaa system. Unlike the blue files available on Kazaa, these files did not breach the applicants' copyrights. However, the court was persuaded by the

---

[86] *Root Quality Pty Ltd v Root Control Technologies Pty Ltd* (2000) 177 ALR 231; 49 IPR 225; [2000] FCA 980 at [146].
[87] Note that the court qualified the test slightly by saying that it would not be limited only to company directors. *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 390.
[88] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 391.
[89] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 391.
[90] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 391.
[91] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 391.
[92] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 392.
[93] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 393.
[94] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 393.
[95] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 393.
[96] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 393.

closeness of the relationship between the Altnet companies and Sharman, the terms of their joint venture agreement and the actual close involvement Altnet had with various aspects of the Kazaa system that the Altnet companies should share Sharman's liability for authorisation of infringement.[97]

Mr Bermeister

Mr Bermeister was President, CEO and one of several directors for Brilliant Digital Entertainment.[98] He was also the sole director (though not owner) of Altnet. Was it appropriate that he share in Sharman's liability?

The principles regarding the circumstances in which Mr Bermeister can be held personally liable for the torts of Altnet and Brilliant Digital Entertainment have been set out above. Applying the test of Finkelstein J in *Root Quality Pty Ltd v Root Control Technologies Pty Ltd* (2000) 177 ALR 231; 49 IPR 225; [2000] FCA 980, the court found that Mr Bermeister played a "key role" in the Altnet-Sharman relationship.[99] It was due to Mr Bermeister's offices that Ms Hemming became involved with Kazaa at all.[100] Upon considering the degree in which Mr Bermeister's involvement influenced the arrangements with Sharman, the court concluded that he was to be held liable for the authorisation of infringement:

> [T]he degree of Mr Bermeister's personal involvement in the acts and omissions of Altnet and BDE, which constitute authorisation of the users' infringing conduct, is such as to render it just to conclude that Mr Bermeister has himself authorised that conduct.[101]

Mr Rose

The final respondent, Mr Rose, is an employee of Brilliant Digital Entertainment. The applicants argued that he should personally share in Sharman's liability.

In the course of his employment Mr Rose was "primarily" responsible for the technical side of Altnet.[102] However, despite this close involvement with the technical aspects of the Kazaa system, the court found no evidence that Mr Rose was "involved in strategic policy decisions or was free to determine whether Altnet should seek to remove from the Kazaa website the material that had the effect of encouraging users to infringe copyright, or to take an active role in countering the users' copyright infringements".[103]

Accordingly, he was not liable for authorisation of users' infringements.

B. The injunction

Collectively Sharman, Ms Hemming, LEF Interactive, Altnet, Brilliant Digital Entertainment and Mr Bermeister will now be referred to as "the infringing respondents".

The court declared that the infringing respondents infringed the copyright in the identified sound recordings by authorising Kazaa users to make copies and communicate the recordings to the public in Australia and by entering into a common design with each other to carry out that authorisation.[104]

The court also declared that there was a risk that further infringement would occur in relation to other sound recordings. Accordingly, it ordered that the infringing respondents be restrained from authorising Kazaa users in Australia to infringe the copyrights in any sound recording belonging to the applicants. However, Wilcox J declared himself "anxious not to make an order which the respondents are not able to obey, except at the unacceptable cost of preventing the sharing even of files which do not infringe the applicants' copyright".[105] This is perhaps a veiled reference to what occurred as a result of the Napster litigation where, despite its best efforts to implement effective filtering technology, Napster was unable to reduce infringements by more than approximately 99%.

---

[97] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 393-396.
[98] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 397.
[99] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 397.
[100] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 397.
[101] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 397.
[102] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 398.
[103] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 399.
[104] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 403.
[105] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 403.

The district court in the case ordered that the Napster service could not come back online until it managed 100% compliance, saying, "It's not good enough until every effort has been made to, in fact, get zero tolerance … There should be no copyright infringement, period."[106] Napster never achieved this target and never went back online. In an effort to avoid a similar situation Wilcox J provided that continuation of the Kazaa system would not be regarded as a violation of the injunction if either Kazaa itself or the Altnet software was modified to implement filtering technology to a standard agreed between the parties or approved by the court.

This order was stayed for a period of two months in order to allow time for a suitable filtering system to be implemented. The order is provisional, with the parties having leave to apply to the court in respect of the form of the orders relating to the injunctions.

In its current form, the injunction orders the infringing respondents to stop authorising Kazaa users to infringe the applicants' copyrights or to implement either keyword filtering technology or gold file flood filtering into the Kazaa software. As the court has recognised, the former will be very difficult, if not impossible, to achieve. Accordingly the infringing respondents will be more or less obliged to choose from the latter two alternatives. These are explained below.

Keyword filtering

The keyword filtering option requires all future versions of the Kazaa software to contain mandatory keyword filtering technology. This is required to be implemented in the next two months so that all new users after that date receive the filtered version of KMD. This option also requires the infringing respondents to place "maximum pressure" on current users to upgrade existing versions of KMD to versions that implement such filtering.

The Kazaa software already contains two discretionary filters that allow users to block executable files (which may contain viruses) and adult content.[107] The proposed keyword filter would be broader and mandatory.

This option requires the applicants and other copyright owners to work together with the infringing respondents to compile a list of song titles and artist names.[108] The infringing respondents are required to change the software so that when a user requests a search, no results that match entries on that list are returned to that user.

Gold file flood filtering

The second option is described as "gold file flood filtering". This takes advantage of the fact that the Kazaa system currently only allows for 200 search results as a result of each search query, as explained in Part 1.

Under this option, a list would also be compiled of copyrighted works and artists. Each time a search requested such a work, the TopSearch component of the Kazaa system would provide 200 results that would include licensed copies of the work and warnings against infringement. This would "flood" the search results with gold file responses, leaving no available space for any unauthorised blue file responses to be sent to the requesting user.

The gold file flood filter alternative is likely to be preferred by the applicants because its effectiveness does not depend on existing users upgrading to a new version of KMD.[109] It simply requires a change to be made to Altnet's TopSearch software. The effect of such a change is that if a user performs a search for a keyword or series of keywords that is on the list, he or she will only receive gold file responses. This remains the case even if the owner of the copyright in the sound recording does not choose to make it commercially available to Kazaa users through the gold file system. In that situation all 200 gold file responses will probably contain warnings against copyright

[106] Eclipse, *A&M Records Inc v Napster Inc - Transcript of Proceedings in United States District Court for the Northern District of California, 11 July 2001*, http://news.findlaw.com/cnn/docs/napster/transcript071101.pdf viewed 30 March 2005, at 32.
[107] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 352.
[108] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 360.
[109] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 368.

infringement. In essence, "all items on the list of copyright works provided by copyright owners become gold file items".[110]

The effect of the injunction

The implementation of either gold file flood filtering or keyword filtering would be likely to significantly reduce the incidence of copyright infringement via the Kazaa system. However, because both options utilise a keyword list to determine what content should be filtered – in the case of keyword filtering to determine whether results should be blocked, and in the case of gold file flood filtering to determine whether gold file results only should be returned to the user – both methods are prone to result in a number of false negatives and false positives.[111]

A false positive might arise if a Jane Smith wanted to distribute her own music via Kazaa, and she shared her name with an artist who was on the list. In that case, any search for "Jane Smith" would result in all matching search results being blocked (under the keyword filtering option) or simply 200 gold file results that included licensed copies of the other Jane Smith's songs (under the gold file flooding option). This problem has the potential to severely compromise the legitimate distribution of music by Kazaa users.

The hypothetical unknown Jane Smith may be able to avoid the problem of false positives under the gold file flood filtering option by contacting Altnet and requesting that her work be listed as a gold file. If she does so, and pays the relevant fee for such a service, any search for "Jane Smith" will then result in her song being returned as a gold file result to the user.[112] However, there is no remedy to the problem of false positives under the keyword filtering option.

False positives are more likely to occur based on song titles than artist names because titles commonly contain generic words such as "love", "angel", or "heart". Accordingly, an authorised copy of a song called "Broken heart" may well be inadvertently caught up by a keyword filter aimed at a different song. Wilcox J considered this possibility. In determining that the risk was acceptable he was heavily influenced by the predominance of unauthorised popular music on the Kazaa system:

> While I accept that a keyword filter would yield some false positives, blocking the sharing of some non-copyright material, there is no evidence that suggests this would be a frequent occurrence. The impression I have gained from the evidence is that the predominant use of the blue files is the sharing of popular music. Such material may be expected to be overwhelmingly subject to copyright.[113]

This is probably the correct view to adopt based on the evidence supplied to the court. There was no evidence giving examples of user searches that would result in false positives.[114] In fact, the applicants submitted that there was "only one example of any person or organisation actually using KMD as a distribution channel, and that example was supported by no examples of any person taking advantage of that availability".[115] On the available evidence, the risk of false positives on the Kazaa system is more hypothetical than real.

False negatives arise when the keyword filter does not recognise a file name as being likely to contain a copyrighted work. Again, because both options involve the use of a keyword list, they are each vulnerable to this problem. For example, the keyword list will contain terms such as "Britney Spears". If a user inaccurately names a file "Britnie Spiers", the keyword filter may not recognise it as being likely to contain a copyrighted work.[116] In most cases false negatives caused by misspellings and inaccurate file names will not concern the applicants. This is because if the file name is sufficiently mangled to avoid the filters, it will also make it difficult for other users to find it via their own searches. However, false negatives can become a problem when users develop new naming

[110] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 368.
[111] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 361.
[112] Evidence was given that such an arrangement had already been offered to Creative Commons content providers. See *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 358.
[113] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 360.
[114] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 360.
[115] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 358.
[116] This will obviously depend on the breadth of the keyword list. It is likely that common misspellings of artist and song names will be included on the list.

conventions designed to systematically evade such filters. This occurred in 2001 when Napster was ordered to implement its own keyword filtering system. Enterprising users got around the system within 24 hours by using a variety of innovative naming conventions such as Pig Latin.[117] For example, instead of "Britney Spears", songs could be found by searching for "itneyBray earsSpay". Once other users were made aware of the naming conventions they were able to search for files with little inconvenience. While keyword lists can be updated to take new names into account, there is nothing to stop users from coming up with still more, potentially beginning a tiresome game of whack-a-mole.[118]

However, expert evidence was given that while some people could use naming conventions to get around the filter, "it would actually be effective for a large percentage of people".[119] That is, most Kazaa users will not bother attempting to try various misspellings and corruptions of the desired song title or artist name to get around the filter. Wilcox J found this acceptable. "I accept any keyword filter will not be totally effective … However, the fact that a protection is imperfect is not a sufficient objection to its adoption."[120]

PART 3. IMPLICATIONS FOR THE AUSTRALIAN LAW OF AUTHORISATION

As indicated in the introduction to this article, the most important issue arising from the decision is the extent to which it indicates to copyright owners and software developers what the latter can and cannot do. Problematically, this message may be conflicting. This section analyses Wilcox J's findings of authorisation and discusses their potential impact on future cases.

A. Authorisation under Australian law

As briefly outlined above, the Act provides that copyright will be infringed where a person who is not the owner or licensee authorises the doing in Australia of any act comprised in the copyright.[121] This requires an infringement or threatened infringement that has actually been authorised by the defendant when he or she was not authorised to do so.

Primary infringements in this instance are not difficult to demonstrate. Kazaa users who made copyrighted files available online were unlawfully exercising the right to communicate a recording to the public under s 85(1)(c) of the Act.[122] Kazaa users who downloaded the files of other users were making unauthorised copies and thus breaching the right to make a copy of the sound recording under s 85(1)(b). The real question was whether Sharman and the other respondents had authorised the Kazaa users to make those copies and communicate the identified recordings to the public.

While the Act has always provided that authorisation in Australia of someone else's copyright infringement also constitutes infringement, no further legislative assistance was provided as to the meaning of authorisation until 2000. Consequently, case law was and still is critical to understanding the meaning of the term. The seminal case regarding authorisation of copyright infringement in Australian law is the High Court decision in *University of New South Wales v Moorhouse* (1975) 133 CLR 1; 49 ALJR 267; 6 ALR 193. That case considered whether a university was liable for authorisation of copyright infringement by virtue of its conduct in placing photocopiers in its libraries and failing to adequately supervise their use in the face of strong evidence that they were being used to infringe copyright.

[117] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 360.
[118] Whack-a-mole or Whac-a-mole is a popular arcade game invented in the 1970s. The game involves a machine with five cut out holes in the top, through which "mole" creatures rapidly pop out and then withdraw their heads. The player aims to hit the mole with a rubber mallet before it goes back into the hole. The term "whack-a-mole" has been used colloquially by computer-related industries to refer to respond to continually recurring miscreants such as senders of spam email.
[119] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 354.
[120] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 361.
[121] *Copyright Act 1968* (Cth) s 101(1).
[122] *Copyright Act 1968* (Cth) s 10 defines "Communicate to the public" as making the recording available online or electronically transmitting it to the public within or outside Australia.

In *Moorhouse* it was held that authorisation occurs where the person has sanctioned, approved, or countenanced the infringement.[123] Such authorisation could occur without direct or positive acts.

> The acts and omissions of the alleged authorizing party must be looked at in the circumstances in which the act comprised in the copyright is done. The circumstances will include the likelihood that such an act will be done. "...[t]he Court may infer an authorization or permission from acts which fall short of being direct and positive; ... indifference, exhibited by acts of commission or omission, may reach a degree from which authorization or permission may be inferred. It is a question of fact in each case what is the true inference to be drawn from the conduct of the person who is said to have authorized …".[124]

Knowledge alone is insufficient to prove authorisation.[125] Equally however, the authorising person need not have knowledge of any specific act of infringement.

> [W]here a general permission or invitation may be implied it is clearly unnecessary that the authorizing party have knowledge that a particular act comprised in the copyright will be done.[126]

B. The controversial "control" requirement

One of the most contentious issues raised during this matter was whether or not some degree of control is necessary in order to make a finding of authorisation and, if so, what should be regarded as sufficient control for the purpose of determining authorisation. In *Moorhouse* Gibbs J considered that the High Court decision in *Adelaide City Corporation v Australasian Performing Right Association Ltd* (1928) 40 CLR 481; 2 ALJR 35; 34 ALR 127 was authority for the proposition that: "A person cannot be said to authorize an infringement of copyright unless he has some power to prevent it."[127]

Useful comments regarding the issue of control were also made by the High Court in *Australian Tape Manufacturers Association Ltd v Commonwealth of Australia* (1993) 176 CLR 480 at 498; 67 ALJR 315; 112 ALR 53; 25 IPR 1.

> It follows that manufacture and sale of articles such as blank tapes or video recorders, which have lawful uses, do not constitute authorization of infringement of copyright, even if the manufacturer or vendor knows that there is a likelihood that the articles will be used for an infringing purpose such as home taping of sound recordings, so long as the manufacturer or vendor has no control over the purchaser's use of the article. It was the absence of such control in [UK House of Lords case *CBS Songs Ltd v Amstrad Consumer Electronics plc* [1988] 1 AC 1013] that constituted the critical distinction between the decision in that case and the decision in Moorhouse, where the University had power to control what was done by way of copying and not only failed to take steps to prevent infringement but provided potential infringers with both the copyright material and the use of the University's machines by which copies of it could be made.

Hence, the High Court was clearly indicating that the sale of a blank tape did not constitute authorization to infringe copyright because the seller could not control the ultimate use of the tape.[128] In other words, the sale of an item of commerce, by itself, has never constituted authorisation in Australia even though that item may be used to infringe copyright. No common law case has ever prohibited the distribution of an item of commerce on the grounds that, after sale, it is capable of being used by its purchaser to infringe copyright. In fact, several cases have said the opposite, namely, that the courts will not prevent such distribution.[129]

---

[123] *University of New South Wales v Moorhouse* (1975) 133 CLR 1 at 12; 49 ALJR 267; 6 ALR 193.
[124] *University of New South Wales v Moorhouse* (1975) 133 CLR 1 at 21; 49 ALJR 267; 6 ALR 193 citing *Adelaide City Corporation v Australasian Performing Right Association Ltd* (1928) 40 CLR 481 at 504; 2 ALJR 35; 34 ALR 127.
[125] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 378 citing *Nationwide News Pty Ltd v Copyright Agency Ltd* (1996) 65 FCR 399 at 422; 136 ALR 273; 34 IPR 53; [1996] AIPC 91-223.
[126] *University of New South Wales v Moorhouse* (1975) 133 CLR 1 at 21; 49 ALJR 267; 6 ALR 193.
[127] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289, at 377 citing *University of New South Wales v Moorhouse* (1975) 133 CLR 1; (1975) 49 ALJR 267; (1975) 6 ALR 193.
[128] *Australian Tape Manufacturers Association Ltd v Commonwealth of Australia* (1993) 176 CLR 480 at 497; 67 ALJR 315; 112 ALR 53; (1993) 25 IPR 1.
[129] See, eg, *CBS Songs Ltd v Amstrad Consumer Electronics plc* (1988) 11 IPR 1 in which case the plaintiffs sought an injunction that would prevent the defendants from selling tape recorders that had copying facilities. In a unanimous decision

In 2000, the Act was amended to provide the following non-exhaustive list of factors that *must be taken into account* when determining whether a person has authorised infringement:

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

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

(c) whether the person took any other reasonable steps to prevent or avoid the doing of the act, including whether the person complied with any relevant industry codes of practice.[130]

Wilcox J noted that the Revised Explanatory Memorandum for the Bill containing this amendment stated that the inclusion of these factors was intended to codify rather than change the principles relating to authorisation of copyright infringement.[131] Accordingly, he accepted that the *Moorhouse* test continued to apply.[132] However, the wording of the first of these codified factors causes some uncertainty. This uncertainty flows from two points relating to its wording.

The first point is that by including the words "(if any)", it suggests that authorisation may exist even where there is no power to prevent the infringement provided that other relevant factors are at work.

The second point arises from the reference to "a power to prevent the doing of the act". Arguably, a power to prevent the doing of the infringing act exists at the time of deciding whether or not to provide the means of infringing copyright. This means that this factor could be interpreted as imposing a requirement to refrain from the distribution of such items. In contrast, an ongoing control over the use of the item (including after the item has been sold or distributed if appropriate) seems to have been the essence of the court's views in *Moorhouse* and the obiter comments in the Australian *Tape Manufacturers' case*. Hence, in the *Moorhouse* decision, the defendant's ongoing control over its photocopying machines was a critical consideration in the finding of authorisation against it. Similarly, in those cases such as *Amstrad* and *Sony*, the sale of an item that could be used for infringing purposes was not itself sufficient to constitute secondary liability. Those cases may have been decided differently if the question was whether it was in their power to prevent their users' infringements at the time they developed their products, rather than whether they had control to prevent those infringements after their products were sold.

The uncertainty surrounding the wording of s 101(1A)(a) was alluded to by Wilcox J himself when he somewhat cryptically noted that: "There may be room for debate as to whether it is desirable to continue to use the word 'control' in this context, having regard to the content of the new subs (1A) of s 101."[133] If it is not "desirable" to continue to use the word "control" in this context, we are almost inevitably led to the conclusion that s 101(1A)(a) has in fact altered and expanded the common law meaning of "authorisation".

Such an approach also has implications for the role and relevance of s 112E. It provides that:

> A person … who provides facilities for making, or facilitating the making of, a communication is not taken to have authorised any infringement of copyright in an audio-visual item merely because another person uses the facilities provided to do something the right to do which is included in the copyright.

The precise meaning of this provision is in question. In particular, what is meant by "merely"? The act of providing the relevant facilities necessarily entails other conduct. For example, the person would presumably have to provide some information explaining what the facilities do. Would the explanation "This software enables sharing of files" go beyond an infringer "merely" infringing the

the House of Lords refused to do so, noting that "In these proceedings the court is being asked to forbid the sale to the public of all or some selected types of tape recorder or to ensure that advertisements for tape recorders shall be censored by the court on behalf of copyright owners. The court has no power to make such orders and judges are not qualified to decide whether a restraint should be placed on the manufacture of electronic equipment or on the contents of advertising": *CBS Songs Ltd v Amstrad Consumer Electronics plc* (1988) 11 IPR 1 at 17.

[130] *Copyright Act 1968* (Cth) s 101(1A).

[131] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 378.

[132] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 385.

[133] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 387.

copyright? Would providing the facilities with such an explanation and seeking a financial advantage from their distribution go beyond an infringer "merely" infringing the copyright? What if the facilities in question are primarily used to infringe copyright although they may have some non-infringing uses?

This issue of interpretation has particular relevance to the first option given to Kazaa in the injunctive relief ordered by Wilcox J. This requires the implementation of mandatory keyword filtering in future versions of KMD and prevents the continued distribution of the original software. In effect, this is an injunction preventing the dissemination of an item of commerce on the grounds that it may be used to infringe copyright. Such an injunction has never before been granted in a common law country. In fact, several previous decisions have expressly and emphatically rejected applications to do so.[134] Perhaps the momentous changes brought about by digital technology and the internet mean that it may now be appropriate to resort to such measures. However, it cannot be denied that to do so requires a fundamental change in the willingness of courts to prevent the distribution of items of commerce, particularly those that may be used for non-infringing purposes.

What is not clear is the extent to which the willingness to grant such a remedy may in turn influence the nature and meaning of authorisation. Wilcox J's determination of liability turned on a combination of factors. However, future defendants will inevitably learn from his decision and alter their conduct accordingly. There will be no exhortations to "Join the Revolution" or even advice that the software can be used to "share" music or films with others. There will be little or no information beyond indicating that the software in question is capable of being used to exchange MP3 files or other types of files. Thus the question will inevitably arise as to whether a defendant has authorised infringement where the only real evidence of authorisation is that they have distributed peer-to-peer software which is capable of being used for infringing purposes.

The wording of s 101(1A)(a) now leaves open the possibility that such action would be sufficient in itself to constitute authorisation. So, in an indirect manner, might the decision in *Kazaa*. If the remedy granted is to prevent the distribution of items of commerce, even though they may be capable of non-infringing uses, the argument will surely be made that consequently the act of authorisation will then be considered to be constituted by the act of distribution of such an item. At that point, copyright becomes the vehicle for the suppression of new technology. Great caution should be exercised before such an outcome is contemplated.

The gold file filtering option referred to in the injunction is not objectionable on this basis. Unlike the keyword filtering option, the gold file filtering option simply requires alteration to what is, in effect, an existing and ongoing indexing service provided by Altnet. The nature of that service is that it demonstrates an ongoing relationship between users and Kazaa and therefore falls squarely within even a narrow view of having "the power to prevent the doing of the act". This part of the injunction is seemingly well within the scope of existing case authority. Curiously, it is also likely to be the preferred option for the copyright industry.

PART IV. KAZAA AND GROKSTER: SECONDARY LIABILITY IN AUSTRALIAN AND UNITED STATES LAW

Prior to delivery of the judgment by Wilcox J, the United States Supreme Court handed down its decision in *MGM Studios v Grokster Ltd* 125 S Ct 2764 (2005). *Grokster* also involved the issue of third party liability for copyright infringements and shared some of the same parties.[135] There were even enormous similarities between the technologies at issue in that case and this – original owners Kazaa BV[136] actually licensed the Kazaa and FastTrack technologies to Grokster and StreamCast

[134] Again see *CBS Songs Ltd v Amstrad Consumer Electronics plc* (1988) 11 IPR 1 at 17.

[135] In both cases, the plaintiffs include some of the largest media companies in the world, and the defendants include Sharman Networks and LEF Interactive. However while they are parties to the main litigation Sharman and LEF Interactive were not involved in the separate application for summary judgment that eventually became the subject of the Supreme Court's decision. For a comprehensive list of all current parties to the litigation, see *MGM Studios Inc v Grokster Ltd* [2005] No 03-55894, No 03-55901, No 03-56236 (Unreported, 9th Cir, 15 August 2005).

[136] Previously known as Consumer Empowerment BV.

Networks, the two respondents to the Supreme Court decision in *Grokster* (the *Grokster* respondents).[137] Yet Wilcox J, in the briefest of comments, simply opined that the decision provided no assistance to him in the application of Australian copyright law to the facts before him. He gave no reason as to why this was so. Given the similarities between the cases, the considered opinions of the American courts on contributory and vicarious liability for copyright infringement may warrant further consideration.

A. The United States law

Until the Supreme Court's decision, liability for copyright infringements by third parties in the United States was believed to be governed by two theories of secondary liability. The Supreme Court's decision held that there was in fact a third theory of liability. This section briefly outlines the three theories and explains how they were applied to the Grokster respondents.

The first theory of secondary liability: Contributory liability

A person will be contributorily liable for a third party's infringement where he or she engaged in conduct that encouraged or assisted the infringement.[138] However, a manufacturer will not be contributorily liable merely for selling a "staple article of commerce" where that product is "capable of substantial noninfringing uses" (the Sony doctrine).[139]

The Sony doctrine was considered in relation to peer-to-peer file sharing for the first time in *A&M Records Inc v Napster Inc* 114 F Supp 2d 896 (ND Cal, 2000) aff'd in part, rev'd in part, 239 F 3d 1004 (9th Cir 2001). Napster was a centralised peer-to-peer network which required users to connect via its own company servers, meaning that if someone at Napster Inc were to turn off a power switch, the network would cease to exist.[140] Napster claimed protection on the basis that, like Sony, it was providing a product that was capable of substantial non-infringing uses. Both the district court and the Ninth Circuit held that where a product is capable of substantial non-infringing uses, the defendant will nonetheless be contributorily liable where it has actual knowledge of the infringement at a time when it is materially contributing to it.[141] Napster not only had ample knowledge of actual infringement, but because it provided the "site and facilities" for direct infringement it materially contributed to that infringement.[142] Accordingly it was likely to be contributorily liable.[143]

The Sony doctrine was reconsidered by the Supreme Court in *Grokster*. The facts and decisions at first instance and on appeal can be set out briefly. The Grokster respondents sought summary judgment from the district court in 2003. The facts were not in issue: they "distributed software that enabled users to exchange digital media via a peer-to-peer transfer network",[144] and in many instances those users did so in breach of copyright.[145] The district court held that it was "undisputed" that the defendant technologies were used for substantial non-infringing purposes, including the distribution of public domain works, authorised music, governmental publications and freely licensed software.[146]

---

[137] "Grokster currently distributes a branded version of the Kazaa Media Desktop, originally licensed by Consumer Empowerment BV (and now controlled by Sharman)": *MGM Studios Inc v Grokster Ltd* 259 F Supp 2d 1029 at 1039 (CD Cal, 2003). Note that StreamCast Networks was formerly known as MusicCity.com Inc. See *MGM Studios Inc v Grokster Ltd* 243 F Supp 2d 1073 at 1080 (CD Cal, 2003).

[138] *A&M Records Inc v Napster Inc* 239 F Supp 3d 1004 at 1019 (9th Cir 2001).

[139] *Sony Corporation of America v Universal City Studios* 464 US 417 at 442-443 (Supreme Court, 1984).

[140] For an excellent description of how Napster operated, see *A&M Records Inc v Napster Inc* 114 F Supp 2d 896 at 905-908 (ND Cal, 2000) aff'd in part, rev'd in part, 239 F 3d 1004 (9th Cir 2001).

[141] *A&M Records Inc v Napster Inc* 239 F Supp 3d 1004 at 1020-1022 (9th Cir 2001).

[142] *A&M Records Inc v Napster Inc*, 239 F Supp 3d 1004 at 1022 (9th Cir 2001).

[143] Note that this decision concerned whether or not an injunction should be granted against Napster Inc and was not the result of a full trial. The court's findings as to Napster's liability for contributory and vicarious liability are that the plaintiffs showed a strong likelihood of success on the merits, the requisite standard for the grant of an injunction. This is a lower standard than is required to succeed at trial, but the matter never went to trial because Napster became bankrupt before the opportunity arose.

[144] *MGM Studios Inc v Grokster Ltd* 259 F Supp 2d 1029 at 1031 (CD Cal, 2003).

[145] *MGM Studios Inc v Grokster Ltd* 259 F Supp 2d 1029 at 1034-1035 (CD Cal, 2003).

[146] *MGM Studios Inc v Grokster Ltd* 259 F Supp 2d 1029 at 1035-1036 (CD Cal, 2003). Note, however, the observation of Ginsburg J in her concurrence that "The District Court's conclusion that '[p]laintiffs do not dispute that Defendants' software is being used, and could be used, for substantial noninfringing purposes,' … is, to say the least, dubious. In the courts below and in this Court, MGM has continuously disputed any such conclusion. Brief for Motion Picture Studio and Recording Company

As the technologies were capable of substantial non-infringing uses, the district court held that "in order to be liable under a theory of contributory infringement, [defendants] must have [had] actual knowledge of infringement at a time when they [could] use that knowledge to stop the particular infringement".[147] The knowledge element was satisfied.[148] The real question was whether that "knowledge of specific infringement accrue[d] at a time when either Defendant materially contribute[d] to the alleged infringement, and [could] therefore do something about it".[149]

As has already been outlined, Grokster and StreamCast initially licensed the KMD software and simply "branded, marketed and distributed" the software.[150] The licence did not include access to the software's source code. This meant that the *Grokster* respondents had no ability whatsoever to change the Kazaa software.[151] "Grokster's primary ability to affect its users' experience derive[d] from its ability to configure a 'start page' and provide advertising automatically retrieved by the Grokster client software."[152] However, StreamCast Networks eventually switched to a different protocol, Gnutella, as the result of a licensing dispute.[153] Both the Kazaa/FastTrack and Gnutella technologies were crafted in such a way that central control was eliminated. This occurred in two ways. First, there was no central server of the type utilised by Napster. Such network structures are commonly referred to as being "decentralised". Second, the defendant Grokster had no control over the content of the software that it distributed because its licence did not provide access to the source code.[154] This meant that Grokster's users could connect to the network, choose which files to share, send and receive searches, and download files, "all with no material involvement of Defendants".[155] Accordingly, the court held that even if it ordered the Grokster respondents to cease having anything to do with their networks, "users of their products could continue sharing files with little or no interruption".[156] This gave rise to a "seminal distinction". Unlike Napster, the Grokster respondents did not provide the "site and facilities" for their users' infringements.[157] As the defendants had no way to use their knowledge of infringement to prevent it, the court held that neither of the Grokster respondents materially contributed to the infringement. On appeal the Ninth Circuit agreed, holding that because substantial non-infringing use was in fact demonstrated, whether or not the "evidence establishes that the vast majority of the software use is for copyright infringement" was irrelevant.[158]

The precise scope and meaning of the Sony doctrine has never been made clear, and there has been much debate over exactly what it means to be "capable of substantial noninfringing uses". When the United States Supreme Court revisited this issue in *Grokster* it became evident that it is itself deeply divided over this issue. Despite unanimously agreeing that the doctrine still applies, the court

Petitioners 30-38; Brief for MGM Plaintiffs-Appellants in No 03-055894, etc (CA9) p 41; App 356-357, 361-365": *MGM Studios Inc v Grokster Ltd* 125 S Ct 2764 at 2786 (2005) (concurrence of Ginsburg J).

[147] *MGM Studios Inc v Grokster Ltd* 259 F Supp 2d 1029 at 1037 (CD Cal, 2003).

[148] *MGM Studios Inc v Grokster Ltd* 259 F Supp 2d 1029 at 1038 (CD Cal, 2003).

[149] *MGM Studios Inc v Grokster Ltd* 259 F Supp 2d 1029 at 1038 (CD Cal, 2003).

[150] *MGM Studios Inc v Grokster Ltd* 243 F Supp 2d 1073 at 1080 (CD Cal, 2003).

[151] *MGM Studios Inc v Grokster Ltd* 259 F Supp 2d 1029 at 1039 (CD Cal, 2003).

[152] *MGM Studios Inc v Grokster Ltd* 259 F Supp 2d 1029 at 1039 (CD Cal, 2003) (internal citation omitted).

[153] "[T]he Streamcast/MusicCity Defendant no longer uses the FastTrack technology. Rather, Streamcast now employs the 'open' (ie, not proprietary) Gnutella networking technology, and distributes its own software instead of a branded version of the Kazaa Media Desktop, which it previously used": *MGM Studios Inc v Grokster Ltd* 243 F Supp 2d 1073 at 1080 (CD Cal, 2003). As Gnutella is open source, anyone with the requisite knowledge could write a client to access the Gnutella network. For the purposes of this article it is not necessary to go into a detailed description of how the Gnutella network operates. It is sufficient to know that like the Kazaa/FastTrack technology it is a decentralised peer-to-peer network. For more information about how it worked at the time StreamCast switched to it, see Oram A, *Gnutella and Freenet Represent True Technological Innovation* http://www.openp2p.com/lpt/a/208 viewed 23 March 2005.

[154] *MGM Studios Inc v Grokster Ltd* 259 F Supp 2d 1029 at 1039 (CD Cal, 2003). Note, however, that StreamCast Networks (once it had switched to the Gnutella network) did have control of its software. However, so did everyone else: the open source nature of the Gnutella network meant that any programmer was free to develop a client to connect to it.

[155] *MGM Studios Inc v Grokster Ltd* 259 F Supp 2d 1029 at 1041 (CD Cal, 2003).

[156] *MGM Studios Inc v Grokster Ltd* 259 F Supp 2d 1029 at 1041 (CD Cal, 2003). However, we note that the gold file flood filtering option may, depending on the agreement between Grokster and Altnet, may have been available.

[157] *MGM Studios Inc v Grokster Ltd* 259 F Supp 2d 1029 at 1041 (CD Cal, 2003).

[158] *MGM Studios Inc v Grokster Ltd* 259 F Supp 2d 1029 at 1062 (CD Cal, 2003).

disagreed regarding what it actually means. Two concurrences to the main *Grokster* opinion, led by Justices Ginsburg and Breyer, illustrate the conflict.

Ginsburg J advocated a narrow interpretation of the doctrine, suggesting that if the *Grokster* matter had to be decided on the basis of presumed intention under *Sony* (rather than the inducement theory) the respondents should not have been granted summary judgment.[159] She argued that

> Even if the absolute number of noninfringing files copied using the Grokster and StreamCast software is large, it does not follow that the products are therefore put to substantial noninfringing uses and are thus immune from liability. The number of noninfringing copies may be reflective of, and dwarfed by, the huge total volume of files shared.[160]

Thus Ginsburg J's concurrence suggests that *Sony* requires an examination of the proportion of infringing to non-infringing uses.

Breyer J, on the other hand, advocates a broader interpretation. He held that Sony protects defendants where their products are in fact capable of being used for substantial non-infringing uses, regardless of the actual level of infringement. On the question whether the *Sony* standard should be given stricter application as suggested by Ginsburg J, Breyer J found that the additional burden of risk and uncertainty that would be caused by Ginsburg J's test "would mean a consequent additional chill of technological development".[161] He recommended the court retain the broad *Sony* standard, leaving it to Congress to address any need for it to be narrowed further.[162]

Two additional judges supported each concurrence. Despite the apparent unanimity of the decision the Supreme Court is deeply divided over *Sony*'s meaning.

The second theory of secondary liability: Vicarious liability

A person will be vicariously liable for a third party's infringement under United States law where he or she had the ability to supervise the infringing activity and a direct financial interest in the infringement.[163]

Napster was held likely to be vicariously liable for the infringements of its users because it had the "right and ability to supervise its users' conduct" by virtue of its indispensable central server through which all search requests were routed.[164]

However, the Grokster respondents avoided vicarious liability because while they clearly had a direct financial interest in the infringement of their users,[165] they had no right or ability to supervise their users' conduct and therefore no obligation to police their networks or implement measures to reduce the infringing conduct.[166]

Accordingly, despite the "possibility that Defendants may have intentionally structured their businesses to avoid secondary liability for copyright infringement, while benefitting [sic] financially from the illicit draw of their wares",[167] the defendants were granted summary judgment. This decision was upheld by the Ninth Circuit,[168] after which the petitioners were given leave to appeal to the Supreme Court.

The third theory of secondary liability: Inducement

On appeal, the Supreme Court unanimously reversed the Ninth Circuit's decision to uphold summary judgment for the defendants. It held that the *Sony* doctrine only operates to preclude a court from presuming intent to cause infringement *solely* on the basis of the design or distribution of a product

[159] *MGM Studios Inc v Grokster Ltd* 125 S Ct 2764 at 2786 (S Ct, 2005) (concurrence of Ginsburg J).
[160] *MGM Studios Inc v Grokster Ltd* 125 S Ct 2764 at 2786 (S Ct, 2005) (concurrence of Ginsburg J).
[161] *MGM Studios Inc v Grokster Ltd*, 125 S Ct 2764 at 2793 (S Ct 2005) (concurrence of Breyer J).
[162] *MGM Studios Inc v Grokster Ltd*, 125 S Ct 2764 at 2796 (S Ct 2005) (concurrence of Breyer J).
[163] See *Gershwin Publishing Corp v Columbia Artists Management Inc* 443 F 2d 1159 at 1162 (2d Cir, 1971).
[164] *A&M Records Inc v Napster Inc* 239 F Supp 3d 1004 at 1023 (9th Cir 2001), citing *A&M Records Inc v Napster Inc* 114 F Supp 2d 896 at 920-921 (ND Cal, 2000) aff'd in part, rev'd in part, 239 F 3d 1004 (9th Cir. 2001).
[165] *MGM Studios Inc v Grokster Ltd* 259 F Supp 2d 1029 at 1043-1044 (CD Cal, 2003).
[166] *MGM Studios Inc v Grokster Ltd* 259 F Supp 2d 1029 at 1044-1045 (CD Cal, 2003).
[167] *MGM Studios Inc v Grokster Ltd* 259 F Supp 2d 1029 at 1046 (CD Cal, 2003).
[168] *MGM Studios Inc v Grokster Ltd* 380 F 3d 1154 (9th Cir, 2004).

that is capable of substantial non-infringing uses.[169] It does not preclude liability where there is *actual* intention to induce infringement.[170] Thus, the *Sony* doctrine protects a defendant from liability unless they have *actually* induced copyright infringement. Both tests must be satisfied to avoid liability.

The Supreme Court did not itself apply the new test, instead remanding the case back to the district court for disposition. However, the wording of its decision strongly suggests that the Grokster respondents should be held liable for their users' infringements.

B. Lessons from the United States law

The present Australian law on authorisation, while developed independently from American case law, nevertheless deals with the same basic issues as to what is the point at which a third party's activities should render it liable for a primary infringement of copyright. In the Kazaa decision, authorisation was found on the basis of a combination of factors. These factors included:

1. The infringing respondents provided the "facilities" for the infringement;[171]
2. The infringing respondents positively encouraged the infringement when they knew that the files predominantly shared through via Kazaa were infringing.[172] Positive acts included their website promotion of KMD as a file-sharing facility,[173] "exhortations" to users to use KMD and share their files;[174] and promotion of the "Join the Revolution" movement, which is "based on file-sharing, especially of music, and which scorns the attitude of record and movie companies in relation to their copyright works";[175]
3. It was in the infringing respondents' financial interest for there to be increasing file-sharing involving an increasing number of people;[176] and
4. Despite having a capability to introduce filters and an awareness that Kazaa was predominantly being used to facilitate the transfer of infringing files, it failed to do so.[177]

While the first instance decision quite rightly focuses on the combination of these factors to reach the ultimate finding of authorisation against most of the defendants, a number of questions nonetheless remain. What will be the legal effect on future defendants if they eliminate one or more of these factors from their conduct? For example, what will happen to a developer and distributor of peer-to-peer software who expressly eschews use of any words or form of promotion that suggests or encourages users to infringe copyright? What if they simply advertise the software on the basis that it can be used to share files between computers? Are they still required to introduce keyword filtering into their software? In other words, will they be prevented from distributing an item of commerce which has both infringing and non-infringing uses? What if, as was the case with Grokster, they do not have the power to introduce key word filtering because they do not have access to the relevant source code? In those circumstances, they only have two options. They either distribute the software without the filter or they do not distribute it at all. In any event, requiring them to include the filter would be analogous to requiring Sony and Amstrad to produce video and cassette players without recording functions.

Eventually, an Australian court may be asked to answer these questions. It is in the interests of both copyright owners and software developers that they do so now. In doing so, it may be useful to

[169] *MGM Studios Inc v Grokster Ltd* 125 S Ct 2764 at 2778 (S Ct, 2005).
[170] *MGM Studios Inc v Grokster Ltd* 125 S Ct 2764 at 2779 (S Ct, 2005).
[171] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 385.
[172] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 385-386.
[173] See *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 312-314.
[174] See *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 312-314.
[175] See *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289, at 314-315 and 335-336. The Court also noted that "Especially to a young audience, the 'Join the Revolution' website material would have conveyed the idea that it was 'cool' to defy the record companies and their stuffy reliance on their copyrights." *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289, at 386
[176] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289, at 385
[177] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289, at 386

draw upon American jurisprudence bearing on the issues. Such an approach would not require slavish adherence to American principles but, at the very least, some consideration of them would be helpful and appropriate in a globalised world and in relation to an internet related copyright issue in which international borders lose much of their relevance.

Among all of the similarities between the *Kazaa case* and *Grokster*, two are particularly significant. First, the product being distributed in each case was being used primarily for infringing purposes. But while each had non-infringing uses, the actual non-infringing uses were very limited and the defendants were unable to provide few if any actual examples of its non-infringing use. Second, there is evidence in each case that the defendants intended to and did in fact induce users of their software to infringe copyright.

It may well be that the "intention" test espoused by the United States Supreme Court may be of little assistance to Australian law. However, a defendant's intention may well be relevant to the question of whether they have in fact induced others to infringe copyright. That question is almost certainly relevant to factors such as the relationship existing between the defendant and the primary infringer and whether the defendant took any reasonable steps to prevent or avoid the doing of the act.

In any event, at some point, Australian courts are likely to have to respond to the issues raised by the Sony decision and the various interpretations of it provided by the United States Supreme Court in the *Grokster* decision. In doing so, they will need to contemplate whether the meaning of authorisation can extend to one or other of the interpretations of the *Sony* test relating to the distribution of items used to infringe copyright.

PART 5. WHACKING THE MOLE – THE NEED FOR BRIGHT LINE RULES OF AUTHORISATION

Sharman Networks is the most significant authorisation decision in Australia since *Moorhouse*. It finally applies the Australian law regarding authorisation to peer-to-peer file sharing software – a technology that was not even contemplated when the principles relating to authorisation were originally developed.

Given the evidence, the outcome has considerable virtue. The infringing respondents appear to have been acting in bad faith to make as much money as possible from the copyright infringements of their users while they had the power to prevent them from doing so. However, in the course of reaching that decision several vital questions were squarely raised and then left unanswered. These must be addressed by the Full Court to provide certainty to future litigants as well as content, software and manufacturing interests alike.

A. Is it appropriate to require the redesign of the product?

Had the court merely ordered the infringing respondents to substantially reduce or eliminate the incidents of copyright infringement by ensuring that searches for copyright material returned only gold file matches, this decision would have fallen well within the scope of longstanding precedent. However, the court's alternative requirement, which requires the infringing respondents to actually alter their product (by implementing keyword filtering) and to cease distributing the unaltered version, is troubling.

The court has essentially required an item of commerce used for infringing and non-infringing uses to be redesigned to reduce or eliminate those infringing uses. This is analogous to allowing the sale of only those VCRs that do not offer a recording function. Such an outcome suggests that the innovation-protecting principles espoused in *Sony* and *Amstrad*, long cited with approval by the Australian High Court, have no further application in the Australian copyright law. Does this mean that content interests can bring litigation against CD burner and media manufacturers or is the decision limited to peer-to-peer technologies? Does it apply to different types of software? If there is a distinction, what is the basis for it? This must be clarified or is likely to cause a chill to technological innovation and investment in Australia.

B. Is "control" necessary for a finding of authorisation?

The Full Court must answer this question by authoritatively determining what exactly s 101(1A) actually means. The language certainly suggests that the existence or otherwise of control is not

decisive, but that contradicts with the legislative history of the provision.[178] Wilcox J declined to answer it on the basis that he considered the infringing respondents did have some control over their software, but the Full Court should deny itself that luxury in order to clarify the uncertainty the decision introduced.

If control is not a necessary factor, software providers and manufacturers will need to know what sort of behaviour would be sufficient to constitute authorisation. That is, how would it be possible to "sanction, approve or countenance" someone else's infringement without having any control over it?

If control is a necessary factor this signals a possible loophole in the Australian law. Like the United States law prior to the Supreme Court's decision in *Grokster*, it would mean that no matter how culpably a provider acted, if it does not have the ability to alter its software it could not be liable for authorisation. As the decision stands it is unclear whether the respondents' liability hinged simply on the fact that they had access to Kazaa's source code. If it did, this is a simple enough factor for future developers to eliminate. In an era of increasingly decentralised technologies this leaves a hole in the Australian copyright law that the legislature must choose whether to plug.

C. What is the meaning of s 112e?

Service providers are explicitly protected by s 112E of the Act. It provides that they are not liable for authorisation merely for providing facilities for making or facilitating the making of communications. The court noted that this meant that in order for a service provider to be liable for authorisation, they must have done something more than "merely" provide the facility that enabled the infringement.[179] However, it is difficult to envisage a situation where a service provider is "merely" making facilities available. At a minimum, those facilities will almost certainly come with some sort of explanation or instruction.

In order to provide certainty to service providers and future litigants it is desirable that the Full Court consider whether or not a bare explanation or instruction accompanying such facilities would alone be sufficient to make a service provider lose the protection of s 112E, or whether the "something more" that is necessary must extend further than factors merely ancillary to the provision of that service.

D. Final words

The importance of clarifying these issues and instituting "bright line" tests for authorisation can be demonstrated by briefly considering the effect of the decision on the Kazaa service itself. When this litigation was first instituted Kazaa posed a major threat to the applicants. It had been downloaded literally hundreds of millions of times.[180] It facilitated the transfer of billions of files each month.[181] In

[178] Previous case law has suggested that control is in fact necessary. See, eg, *Australian Tape Manufacturers Association Ltd v Commonwealth of Australia* (1993) 176 CLR 480 at 498; 67 ALJR 315; 112 ALR 53; 25 IPR 1: "It follows that manufacture and sale of articles such as blank tapes or video recorders, which have lawful uses, do not constitute authorization of infringement of copyright, even if the manufacturer or vendor knows that there is a likelihood that the articles will be used for an infringing purpose such as home taping of sound recordings, *so long as the manufacturer or vendor has no control over the purchaser's use of the article. It was the absence of such control in [Amstrad] that constituted the critical distinction between the decision in that case and the decision in Moorhouse, where the University had power to control what was done by way of copying and not only failed to take steps to prevent infringement but provided potential infringers with both the copyright material and the use of the University's machines by which copies of it could be made*" (footnotes omitted, emphasis added). The legislation specifically stated that it was intended to codify the common law. See *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 378.

[179] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 385.

[180] "At the beginning of 2004, the Kazaa website was claiming that over 2.4 million people downloaded the Kazaa software during the previous week; that is, there were over 2.4 million new users that week. The KMD webpage claimed total downloads of 317,552,315 people. That figure equates to about 5% of the world's human population": *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 337.

[181] Altnet, one of the respondents held liable for authorisation of copyright infringement, claimed that Kazaa's 60 million users downloaded over three billion files each month: *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 147. Wilcox J noted that while it was theoretically possible for the system to be used to transfer non-infringing files, "in May 2003, Kazaa was being predominantly used for music file-sharing. A reader who had even a general understanding of copyright law would also have realised this necessarily involved copyright infringement on a massive scale": *Universal Music*

2003, it was used for 79% of global peer-to-peer file sharing.[182] But in the time it has taken for the service to be investigated, its corporate structure untangled, litigation instituted, the matter heard and finally a ruling to be made by the court, Kazaa has essentially become almost irrelevant in the world of peer-to-peer file sharing. A recent study by Britain-based research firm CacheLogic suggested that the Kazaa network is now only responsible for around 10% of peer-to-peer traffic, despite that traffic growing enormously to now constitute around 60% of all internet traffic.[183]

Almost certainly this decision will be effective to end what copyright infringement still occurs via Kazaa software. But the absence of bright line tests for authorisation meant that it was impossible to act quickly to obtain a ruling while it still had some relevance. If the Full Court does not clarify the tests relating to authorisation upon this appeal, the situation will be repeated the next time. As any child at a carnival knows, there's no prize for whacking the mole after five others have popped their heads up.

Australia Pty Ltd v Sharman License Holdings Ltd (2005) 65 IPR 289 at 337. Accordingly it is appropriate to surmise that the number of unauthorised transfers of copyrighted material each month amounted to billions.

[182] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 at 332.

[183] *Kazaa hit by file-sharing ruling* http://news.bbc.co.uk/2/hi/technology/4214810.stm viewed 15 September 2005.