Federal Court of Australia

[Index] [Search] [Download] [Help]

Universal Music Australia Pty Ltd v Sharman License Holdings Ltd (with Corrigendum dated 22 September 2005) [2005] FCA 1242 (5 September 2005)

Last Updated: 30 September 2005

FEDERAL COURT OF AUSTRALIA

Universal Music Australia Pty Ltd v Sharman License Holdings Ltd [2005] FCA 1242

CORRIGENDUM

UNIVERSAL MUSIC AUSTRALIA PTY LTD, FESTIVAL RECORDS PTY LTD AND MUSHROOM RECORDS PTY LTD TRADING AS FESTIVAL MUSHROOM RECORDS, EMI MUSIC AUSTRALIA PTY LIMITED, SONY MUSIC ENTERTAINMENT (AUSTRALIA) LIMITED, WARNER MUSIC AUSTRALIA PTY LIMITED, BMG AUSTRALIA LIMITED, UMG RECORDS, INC., SHADY RECORDS, INC./INTERSCOPE RECORDS, AFTERMATH RECORDS, REAL HORRORSHOW PTY LTD, THE LIVING END PTY LTD, VIRGIN RECORDS AMERICA, INC, EMI RECORDS LTD, CAPITOL RECORDS, INC, ARISTA RECORDS, LLC (FORMERLY KNOWN AS ARISTA RECORDS, INC.), CIRCA RECORDS LTD, CHRYSALIS RECORDS LTD, SONY MUSIC (AUSTRALIA) PTY LTD, SONY MUSIC ENTERTAINMENT (CANADA) INC., SONY BMG MUSIC ENTERTAINMENT, MAYER MUSIC LLC, TIMOTHY JAMES FREEDMAN, WARNER BROS. RECORDS, INC., ATLANTIC RECORDING CORPORATION,

WARNER MUSIC UK LTD, J RUBY PRODUCTIONS, INC. DBA SLASH RECORDS, ZOMBA RECORDING LLC (FORMERLY KNOWN AS ZOMBA RECORDING CORPORATION), BMG MUSIC (BMG MUSIC DBA THE RCA RECORDS LABEL, A UNIT OF BMG ENTERTAINMENT), BMG UK & IRELAND LTD, LAFACE RECORDS v SHARMAN LICENSE HOLDINGS LTD, SHARMAN NETWORKS LTD, LEF INTERACTIVE PTY LTD, NICOLA ANNE HEMMING, PHILIP MORLE, ALTNET INC, BRILLIANT DIGITAL ENTERTAINMENT INC, BRILLIANT DIGITAL ENTERTAINMENT PTY LTD, KEVIN GLEN BERMEISTER, ANTHONY ROSE

NSD 110 of 2004

WILCOX J
5 SEPTEMBER 2005 (CORRIGENDUM 22 SEPTEMBER 2005)
SYDNEY

IN THE FEDERAL COURT OF AUSTRALIA
NEW SOUTH WALES DISTRICT REGISTRY **NSD 110 of 2004**

BETWEEN: **UNIVERSAL MUSIC AUSTRALIA PTY LTD**
FIRST APPLICANT

FESTIVAL RECORDS PTY LTD AND MUSHROOM RECORDS PTY LTD TRADING AS FESTIVAL MUSHROOM RECORDS
SECOND APPLICANT

EMI MUSIC AUSTRALIA PTY LIMITED
THIRD APPLICANT

SONY MUSIC ENTERTAINMENT (AUSTRALIA) LIMITED
FOURTH APPLICANT

WARNER MUSIC AUSTRALIA PTY LIMITED
FIFTH APPLICANT

BMG AUSTRALIA LIMITED
SIXTH APPLICANT

UMG RECORDS, INC.
SEVENTH APPLICANT

SHADY RECORDS, INC./INTERSCOPE RECORDS
EIGHTH APPLICANT

AFTERMATH RECORDS
NINTH APPLICANT

REAL HORRORSHOW PTY LTD
TENTH APPLICANT

THE LIVING END PTY LTD
ELEVENTH APPLICANT

VIRGIN RECORDS AMERICA, INC
TWELFTH APPLICANT

EMI RECORDS LTD
THIRTEENTH APPLICANT

CAPITOL RECORDS, INC
FOURTEENTH APPLICANT

ARISTA RECORDS, LLC (FORMERLY KNOWN AS ARISTA RECORDS, INC.)
FIFTEENTH APPLICANT

CIRCA RECORDS LTD
SIXTEENTH APPLICANT

CHRYSALIS RECORDS LTD
SEVENTEENTH APPLICANT

SONY MUSIC (AUSTRALIA) PTY LTD
EIGHTEENTH APPLICANT

SONY MUSIC ENTERTAINMENT (CANADA) INC.
NINETEENTH APPLICANT

SONY BMG MUSIC ENTERTAINMENT
TWENTIETH APPLICANT

MAYER MUSIC LLC
TWENTY-FIRST APPLICANT

TIMOTHY JAMES FREEDMAN
TWENTY-SECOND APPLICANT

WARNER BROS. RECORDS, INC.
TWENTY-THIRD APPLICANT

ATLANTIC RECORDING CORPORATION
TWENTY-FOURTH APPLICANT

WARNER MUSIC UK LTD
TWENTY-FIFTH APPLICANT

J RUBY PRODUCTIONS, INC. DBA SLASH RECORDS
TWENTY-SIXTH APPLICANT

ZOMBA RECORDING LLC (FORMERLY KNOWN AS ZOMBA RECORDING CORPORATION)
TWENTY-SEVENTH APPLICANT

BMG MUSIC (BMG MUSIC DBA THE RCA RECORDS LABEL, A UNIT OF BMG ENTERTAINMENT)
TWENTY-EIGHTH APPLICANT

BMG UK & IRELAND LTD
TWENTY-NINTH APPLICANT

LAFACE RECORDS
THIRTIETH APPLICANT

AND: **SHARMAN LICENSE HOLDINGS LTD**
FIRST RESPONDENT

SHARMAN NETWORKS LTD
SECOND RESPONDENT

LEF INTERACTIVE PTY LTD
THIRD RESPONDENT

NICOLA ANNE HEMMING
FOURTH RESPONDENT

PHILIP MORLE
FIFTH RESPONDENT

ALTNET INC
SIXTH RESPONDENT

BRILLIANT DIGITAL ENTERTAINMENT INC
SEVENTH RESPONDENT

BRILLIANT DIGITAL ENTERTAINMENT PTY LTD
EIGHTH RESPONDENT

KEVIN GLEN BERMEISTER
NINTH RESPONDENT

ANTHONY ROSE

TENTH RESPONDENT

JUDGE: **WILCOX J**

DATE OF ORDER: **5 SEPTEMBER 2005 (CORRIGENDUM 22 SEPTEMBER 2005)**

WHERE MADE: **SYDNEY**

CORRIGENDUM

1. At page 143, paragraph 449 in the Reasons for Judgment of the Honourable Justice Wilcox delivered on 5 September 2005, delete the last sentence which reads:

'There is no material that rebuts, and I see reason to reject, this evidence.'

And replace with:
'There is no material that rebuts, and I see no reason to reject, this evidence.'

I certify that the preceding one (1) numbered paragraph is a true copy of the Corrigendum to the Reasons for Judgment of the Honourable Justice Wilcox.

Associate
22 September 2005

FEDERAL COURT OF AUSTRALIA

Universal Music Australia Pty Ltd v Sharman License Holdings Ltd

[2005] FCA 1242

SUMMARY

UNIVERSAL MUSIC AUSTRALIA PTY LTD & ORS v SHARMAN LICENSE HOLDINGS LTD & ORS
NSD 110 OF 2004

WILCOX J
SYDNEY
5 SEPTEMBER 2005

SUMMARY

In accordance with the practice of the Federal Court in certain cases of public interest, the Court has prepared a summary to accompany the judgment that is to be delivered today. However, it must be emphasised that the summary forms no part of the judgment. The only authoritative statement of the Court's reasons is the judgment itself.

This summary is intended to assist in understanding the principal conclusions reached by the Court, but it is necessarily incomplete. The published reasons for judgment and this summary will be available on the internet www.fedcourt.gov.au.

Universal Music Australia Pty Ltd v Sharman License Holdings Ltd

[2005] FCA 1242

I am about to deliver judgment in a case that has attracted widespread interest. Extensive evidence was presented at the trial. Much of it was of a technical nature. The facts of the case and the relevant law are both complex. My reasons for judgment are, therefore, necessarily lengthy. Because of those factors, I have prepared this statement in which I will attempt briefly to explain the nature of the case and my major conclusions. This statement is not intended comprehensively to set out my findings of fact, conclusions about the law or reasons for making the orders I will shortly announce. Those interested in obtaining full information about those matters should refer to the Court's website (www.fedcourt.gov.au), upon which my full Reasons for Decision will shortly be published.

The case concerns the operation of the Kazaa Internet peer-to-peer file-sharing system. This system operates world wide. Since early 2002, it has been controlled by Sharman Networks Ltd, one of the present respondents, out of premises in Sydney. Four of the other respondents are directly associated with Sharman Networks.

The Kazaa system is available to users free of charge. It enables one user to share with other users any material the first user wishes to share, whether or not that material is subject to copyright, simply by placing that material in a file called 'My Shared Folder'. A user who is interested in obtaining a copy of a particular work, such as a musical item, can instantaneously search the 'My Shared Folder' files of other users, worldwide. If the file is located, the title will be displayed against a blue icon on the first user's computer as a 'blue file'. The work can then be downloaded onto the first user's computer. The technology used to carry out those operations is called FastTrack.

Shortly after Sharman Networks took control of Kazaa, the system was expanded so as to add a second type of search. This was done by arrangement with Altnet Inc, a United States company which is also a respondent in this case. Four other respondents are associated with Altnet.

Altnet controlled technology called TopSearch, which enables the provision to Kazaa users of licensed works; that is, works made available to users pursuant to arrangements made with the owners of the copyright in those works. Search results for these works are displayed on a user's computer against a gold icon; they have been called 'gold files'.

There are 30 applicants in this case. They include companies associated with the world's major distributors of sound recordings, mostly in the form of compact discs. The applicants claim the sharing of blue files between users constitutes an infringement of their copyright. They do not contend the sharing of gold files directly infringes their copyright. However, they have joined the Altnet parties because, they say, the arrangements made between the Sharman parties and the Altnet parties constitute a joint enterprise; so all

the respondents are involved in the relevant infringements of copyright. Also, they say, Altnet personnel assisted Sharman personnel in constructing the Kazaa website, which contains material encouraging users to infringe copyright in blue file works.

The Kazaa system is extremely popular. Documents produced by the respondents contain claims that, at any particular time, several million people are using the system to share files. At the beginning of 2004, the Kazaa website said over 317 million people, worldwide, had downloaded Kazaa onto their computers, thereby enabling them to share files. A banner on the Kazaa website, at the time of the commencement of this proceeding, claimed Kazaa was '[t]he world's most downloaded software application'. A document produced by the respondents stated that Kazaa was used for 79% of worldwide peer-to-peer file-sharing activities.

It is clear that a major proportion of Kazaa's shared blue files are works (mostly musical works) that are subject to copyright. The files are shared without the approval of the relevant copyright owner. It follows that both the user who makes the file available and the user who downloads a copy infringes the owner's copyright.

In this case, the applicants made claims of copyright infringement, contravention of the *Trade Practices Act* and conspiracy. It is convenient to say immediately that the evidence does not support either the *Trade Practices Act* or conspiracy claims. Those claims will be rejected. The more arguable claim is infringement of the applicants' copyright.

Before I indicate my conclusions about that claim, I wish to identify two matters that this case is **not** about.

First, many people (including the respondents) argue that the Internet is here to stay, it is being used by an ever increasing number of people and peer-to-peer file-sharing is one of its most valuable potential uses. They say that copyright owners, such as the present applicants, could eliminate (or at least substantially reduce) infringement of their copyrights if they were willing to make copyright works available on a licensed basis for a fee, in the way in which Altnet offers gold files. Second, it was suggested at one stage of this case that it would have been possible for the applicants to have made their compact discs less vulnerable to being 'ripped' into a computer program by issuing them in a digital rights managed, rather than open, format.

Neither of these matters fall for decision in this case. I understand the argument in favour of more widespread licensing of copyright works. No doubt that course would have commercial implications for sound recording distributors. Whether or not they should take it is a matter to be determined by them. Unless and until they do decide to take that course, they are entitled to invoke such protective rights as the law affords them. Similarly in regard to making compact discs less susceptible to ripping; although, in regard to that matter, I add the evidence is insufficient for me to reach any conclusion about the feasibility of doing this.

I return to the true issue in the case: the applicants' copyright claim. Here again, the applicants overstated their case. It cannot be concluded, as the applicants claimed in their pleadings, that the respondents themselves engaged in communicating the applicants' copyright works. They did not do so. The more realistic claim is that the respondents authorised users to infringe the applicants' copyright in their sound recordings. Section 101 of the Australian *Copyright Act* provides that copyright is infringed by a person who, not being the owner of the copyright and without the licence of the copyright owner, authorises another person to do in Australia an infringing act.

I have concluded that this more limited claim is established against six of the ten respondents. My reasons may be summarised in this way:

> (i) despite the fact that the Kazaa website contains warnings against the sharing of copyright files, and an end user licence agreement under which users are made to agree not to infringe copyright, it has long been obvious that those measures are ineffective to prevent, or even substantially to curtail, copyright infringements by users. The respondents have long known that the Kazaa system is widely used for the sharing of copyright files;
> (ii) there are technical measures (keyword filtering and gold file flood filtering) that would enable the respondents to curtail – although probably not totally to prevent – the sharing of copyright files. The respondents have not taken any action to implement those measures. It would be against their financial interest to do so. It is in the respondents' financial interest to maximise, not to minimise, music file-sharing. Advertising provides the bulk of the revenue earned by the Kazaa system, which revenue is shared between Sharman Networks and Altnet.
> (iii) far from taking steps that are likely effectively to curtail copyright file-sharing, Sharman Networks and Altnet have included on the Kazaa website exhortations to users to increase their file-sharing and a webpage headed 'Join the Revolution' that criticises record companies for opposing peer-to-peer file-sharing. They also sponsored a 'Kazaa Revolution' campaign attacking the record companies. The revolutionary material does not expressly advocate the sharing of copyright files. However, to a young audience, and it seems that Kazaa users are predominantly young people, the effect of this webpage would be to encourage visitors to think it 'cool' to defy the record companies by ignoring copyright constraints.

A question arose as to the form of relief that might be made against the six respondents that I hold to have authorised infringement of the applicants' copyright. The applicants are entitled to declarations as to past violations of their rights and the threat of future violations. They are also entitled to an order restraining future violations. However, I have had to bear in mind the possibility that, even with the best will in the world, the respondents probably cannot totally prevent copyright infringement by users. I am 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. There needs to be an opportunity for the relevant respondents to modify the Kazaa system in a targeted way, so as to protect the applicants' copyright interests (as far as possible) but without unnecessarily intruding on others' freedom of speech and communication. The evidence about keyword filtering and gold file flood filtering, indicates how this might be done. It should be provided that the injunctive order will be satisfied if the respondents take either of these steps. The steps, in my judgment, are available to the respondents and likely significantly, though perhaps not totally, to protect the applicants' copyrights.

The formal orders that I make are as follows:

> 1. Leave be granted to Australian Consumers' Association Pty Ltd, Electronic Frontiers Australia Inc and New South Wales Council for Civil Liberties Inc to intervene in this proceeding to the extent necessary for them to put submissions that do not depend on material not already in evidence.
>
> 2. It be declared that each of the six respondents named below ('the infringing respondents') have infringed the copyright in each of the sound recordings whose title appears in column 2 of the attached Schedule, being a copyright of the applicant ('the relevant applicant') whose name

is set out opposite the title of that sound recording in column 4 of that Schedule by:

> (i) authorising the doing in Australia by Kazaa users of the following acts ('the infringing acts') in relation to the said sound recording:
> (a) making a copy of the sound recording;
>
> (b) communicating the recording to the public;
>
> in each case, without the licence of the relevant applicant; and
> (ii) entering into a common design, with each of the other infringing respondents, to carry out, procure or direct the said authorisation;

The infringing respondents are Sharman Networks Ltd, LEF Interactive Pty Ltd, Nicola Anne Hemming, Altnet Inc, Brilliant Digital Entertainment Inc and Kevin Glen Bermeister.

3. It be declared that each of the infringing respondents threatens to infringe the copyright of the applicants in other sound recordings by:

> (i) authorising the doing in Australia by Kazaa users of the infringing acts; in each case, without the licence of the applicant who is the relevant copyright owner; and
> (ii) entering into a common design with each of the other infringing respondents, to carry out, procure or direct the said authorisation.

4. The infringing respondents be restrained, by themselves, their servants or agents, from authorising Kazaa users to do in Australia any of the infringing acts, in relation to any sound recording of which any of the applicants is the copyright owner, without the licence of the relevant copyright owner.

5. Continuation of the Kazaa Internet file-sharing system (including the provision of software programs to new users) shall not be regarded as a contravention of order 4 if that system is first modified pursuant to a protocol, to be agreed between the infringing respondents and the applicants or to be approved by the Court, that ensures either of the following situations:

> (i): that:
>
> > (a) the software program received by all new users of the Kazaa file-sharing system contains non-optional key-word filter technology that excludes from the displayed blue file search results all works identified (by titles, composers' or performers' names or otherwise) in such lists of their copyright works as may be provided, and periodically updated, by any of the applicants; and
> > (b) all future versions of the Kazaa file-sharing system contain the said non-optional key-word filter technology; and
> > (c) maximum pressure is placed on existing users, by the use of dialogue boxes on the Kazaa website, to upgrade their existing Kazaa software program to a new version of the program containing the said non-optional key-word filter technology; or

(ii) that the TopSearch component of the Kazaa system will provide, in answer to a request for a work identified in any such list, search results that are limited to licensed works and warnings against copyright infringement and that will exclude provision of a copy of any such identified work.

6. The operation of order 4 be stayed for a period of two months from today's date, or for such extended period as a judge may, on application, allow.

7. The applicants' claims for pecuniary relief against the infringing respondents be reserved for determination at a hearing to be fixed on application for that purpose.

8. There be liberty to all parties to apply, on seven days notice:

(a) within a period of one month from today's date, in respect of the form of order 4 or 5;
(b) generally, in respect of any Court approval required for the purposes of order 5, or any order required for purposes related to order 6 or order 7.

9. The applicants' claims under the *Trade Practices Act 1974* (Cth), the *Fair Trading Act 1987* (NSW) and in respect of the tort of conspiracy all be dismissed.

10. The infringing respondents pay 90% of the costs incurred by the applicants to date in relation to this proceeding.

11. The proceeding be wholly dismissed as against the following four respondents ('the dismissed respondents'): Sharman License Holdings Ltd, Philip Morle, Brilliant Digital Entertainment Pty Ltd and Anthony Rose.

12. The applicants pay the costs incurred in relation to this proceeding by each of the dismissed respondents, provided that, in the case of those dismissed respondents who were represented at the trial jointly with infringing respondents, such costs shall be limited to costs other than those that would have been incurred, in any event, in connection with representation of the relevant infringing respondents.

Wilcox J
Sydney
5 September 2005

FEDERAL COURT OF AUSTRALIA

Universal Music Australia Pty Ltd v Sharman License Holdings Ltd [2005] FCA 1242

COPYRIGHT – Authorisation – Internet file-sharing – Suit by owners of copyright in sound recordings

against parties involved with Kazaa peer-to-peer file sharing system – Whether respondents authorised infringements of copyright by Kazaa users – Issues as to respondents' knowledge of, and intentions concerning, users' activities – Extent of respondents' control of those activities – Whether Kazaa system includes a central server – Termination, filtering and other technological controls – Non-technological controls – Whether the respondents merely provided the facilities used by Kazaa users – Application of s 101 of *Copyright Act* to each respondent.

TRADE PRACTICES – Alleged misleading and deceptive conduct.

CONSPIRACY – Alleged combination – Whether sole or dominant purpose to injure applicants – Whether agreement to use unlawful means to injure applicants.

Copyright Act 1968 (Cth) ss 10, 13(2), 22(6), 85, 101, 112E
Trade Practices Act 1974 (Cth) ss 52, 52A

WEA International Inc v Hanimex Corporation Ltd (1987) 17 FCR 274 considered
University of New South Wales v Moorhouse (1975) 133 CLR 1 considered and applied
CBS Songs Ltd v Amstrad Consumer Electronics PLC [1988] 1 AC 1013 distinguished
Australian Tape Manufacturers Association Ltd v Commonwealth of Australia (1993) 176 CLR 480 considered
Australasian Performing Right Association Ltd v Metro on George Pty Ltd (2004) 61 IPR 575 followed
Australasian Performing Right Association Ltd v Jain (1990) 26 FCR 53 applied
King v Milpurrurra (1996) 66 FCR 474 considered
Microsoft Corporation v Auschina Polaris Pty Ltd (1996) 71 FCR 231 followed
Root Quality Pty Ltd v Root Control Technologies Pty Ltd 177 ALR 231 applied

UNIVERSAL MUSIC AUSTRALIA PTY LTD, FESTIVAL RECORDS PTY LTD AND MUSHROOM RECORDS PTY LTD TRADING AS FESTIVAL MUSHROOM RECORDS, EMI MUSIC AUSTRALIA PTY LIMITED, SONY MUSIC ENTERTAINMENT (AUSTRALIA) LIMITED, WARNER MUSIC AUSTRALIA PTY LIMITED, BMG AUSTRALIA LIMITED, UMG RECORDS, INC., SHADY RECORDS, INC./INTERSCOPE RECORDS, AFTERMATH RECORDS, REAL HORRORSHOW PTY LTD, THE LIVING END PTY LTD, VIRGIN RECORDS AMERICA, INC, EMI RECORDS LTD, CAPITOL RECORDS, INC, ARISTA RECORDS, LLC (FORMERLY KNOWN AS ARISTA RECORDS, INC.), CIRCA RECORDS LTD, CHRYSALIS RECORDS LTD, SONY MUSIC (AUSTRALIA) PTY LTD, SONY MUSIC ENTERTAINMENT (CANADA) INC., SONY BMG MUSIC ENTERTAINMENT, MAYER MUSIC LLC, TIMOTHY JAMES FREEDMAN, WARNER BROS. RECORDS, INC., ATLANTIC RECORDING CORPORATION, WARNER MUSIC UK LTD, J RUBY PRODUCTIONS, INC. DBA SLASH RECORDS, ZOMBA RECORDING LLC (FORMERLY KNOWN AS ZOMBA RECORDING CORPORATION), BMG MUSIC (BMG MUSIC DBA THE RCA RECORDS LABEL, A UNIT OF BMG ENTERTAINMENT), BMG UK & IRELAND LTD, LAFACE RECORDS v SHARMAN LICENSE HOLDINGS LTD, SHARMAN NETWORKS LTD, LEF INTERACTIVE PTY LTD, NICOLA ANNE

HEMMING, PHILIP MORLE, ALTNET INC, BRILLIANT DIGITAL ENTERTAINMENT INC, BRILLIANT DIGITAL ENTERTAINMENT PTY LTD, KEVIN GLEN BERMEISTER, ANTHONY ROSE

NSD 110 of 2004

WILCOX J
5 SEPTEMBER 2005
SYDNEY

IN THE FEDERAL COURT OF AUSTRALIA
NEW SOUTH WALES DISTRICT REGISTRY **NSD 110 of 2004**

BETWEEN: **UNIVERSAL MUSIC AUSTRALIA PTY LTD**
FIRST APPLICANT

FESTIVAL RECORDS PTY LTD AND MUSHROOM RECORDS PTY LTD TRADING AS FESTIVAL MUSHROOM RECORDS

SECOND APPLICANT

EMI MUSIC AUSTRALIA PTY LIMITED
THIRD APPLICANT

SONY MUSIC ENTERTAINMENT (AUSTRALIA) LIMITED
FOURTH APPLICANT

WARNER MUSIC AUSTRALIA PTY LIMITED
FIFTH APPLICANT

BMG AUSTRALIA LIMITED
SIXTH APPLICANT

UMG RECORDS, INC.
SEVENTH APPLICANT

SHADY RECORDS, INC./INTERSCOPE RECORDS
EIGHTH APPLICANT

AFTERMATH RECORDS
NINTH APPLICANT

REAL HORRORSHOW PTY LTD
TENTH APPLICANT

THE LIVING END PTY LTD
ELEVENTH APPLICANT

VIRGIN RECORDS AMERICA, INC
TWELFTH APPLICANT

EMI RECORDS LTD
THIRTEENTH APPLICANT

CAPITOL RECORDS, INC
FOURTEENTH APPLICANT

ARISTA RECORDS, LLC (FORMERLY KNOWN AS ARISTA RECORDS, INC.)
FIFTEENTH APPLICANT

CIRCA RECORDS LTD
SIXTEENTH APPLICANT

CHRYSALIS RECORDS LTD
SEVENTEENTH APPLICANT

SONY MUSIC (AUSTRALIA) PTY LTD
EIGHTEENTH APPLICANT

SONY MUSIC ENTERTAINMENT (CANADA) INC.
NINETEENTH APPLICANT

SONY BMG MUSIC ENTERTAINMENT
TWENTIETH APPLICANT

MAYER MUSIC LLC
TWENTY-FIRST APPLICANT

TIMOTHY JAMES FREEDMAN
TWENTY-SECOND APPLICANT

WARNER BROS. RECORDS, INC.
TWENTY-THIRD APPLICANT

ATLANTIC RECORDING CORPORATION
TWENTY-FOURTH APPLICANT

WARNER MUSIC UK LTD
TWENTY-FIFTH APPLICANT

J RUBY PRODUCTIONS, INC. DBA SLASH RECORDS
TWENTY-SIXTH APPLICANT

ZOMBA RECORDING LLC (FORMERLY KNOWN AS ZOMBA RECORDING CORPORATION)
TWENTY-SEVENTH APPLICANT

BMG MUSIC (BMG MUSIC DBA THE RCA RECORDS LABEL, A UNIT OF BMG ENTERTAINMENT)
TWENTY-EIGHTH APPLICANT

BMG UK & IRELAND LTD
TWENTY-NINTH APPLICANT

LAFACE RECORDS
THIRTIETH APPLICANT

AND: **SHARMAN LICENSE HOLDINGS LTD**
FIRST RESPONDENT

SHARMAN NETWORKS LTD
SECOND RESPONDENT

LEF INTERACTIVE PTY LTD
THIRD RESPONDENT

NICOLA ANNE HEMMING
FOURTH RESPONDENT

PHILIP MORLE
FIFTH RESPONDENT

ALTNET INC
SIXTH RESPONDENT

BRILLIANT DIGITAL ENTERTAINMENT INC
SEVENTH RESPONDENT

BRILLIANT DIGITAL ENTERTAINMENT PTY LTD
EIGHTH RESPONDENT

KEVIN GLEN BERMEISTER
NINTH RESPONDENT

ANTHONY ROSE
TENTH RESPONDENT

JUDGE: **WILCOX J**
DATE OF ORDER: **5 SEPTEMBER 2005**
WHERE MADE: **SYDNEY**

THE COURT ORDERS THAT:

1. Leave be granted to Australian Consumers' Association Pty Ltd, Electronic Frontiers Australia Inc and New South Wales Council for Civil Liberties Inc to intervene in this proceeding to the extent necessary for them to put submissions that do not depend on material not already in evidence.

2. It be declared that each of the six respondents named below ('the infringing respondents') have infringed the copyright in each of the sound recordings whose title appears in column 2 of the attached Schedule, being a copyright of the applicant ('the relevant applicant') whose name is set out in the same row as the title of that sound recording in column 4 of that Schedule by:

(i) authorising the doing in Australia by Kazaa users of the following acts ('the infringing acts') in relation to the said sound recording:

(a) making a copy of the sound recording;

(b) communicating the recording to the public;
in each case, without the licence of the relevant applicant; and

(ii) entering into a common design, with each of the other infringing respondents, to carry out, procure or direct the said authorisation;

The infringing respondents are Sharman Networks Ltd, LEF Interactive Pty Ltd, Nicola Anne Hemming, Altnet Inc, Brilliant Digital Entertainment Inc and Kevin Glen Bermeister.

3. It be declared that each of the infringing respondents threatens to infringe the copyright of the applicants in other sound recordings by:

(i) authorising the doing in Australia by Kazaa users of the infringing acts; in each case, without the licence of the applicant who is the relevant copyright owner; and
(ii) entering into a common design with each of the other infringing respondents, to carry out, procure or direct the said authorisation.

4. The infringing respondents be restrained, by themselves, their servants or agents, from authorising Kazaa users to do in Australia any of the infringing acts, in relation to any sound recording of which any of the applicants is the copyright owner, without the licence of the relevant copyright owner.

5. Continuation of the Kazaa Internet file-sharing system (including the provision of software programs to new users) shall not be regarded as a contravention of order 4 if that system is first modified pursuant to a protocol, to be agreed between the infringing respondents and the applicants, or to be approved by the Court, that ensures either of the following situations:

(i): that:

(a) the software program received by all new users of the Kazaa file-sharing system contains non-optional key word filter technology that excludes from the displayed blue file search results all works identified (by titles, composers' or performers' names or otherwise) in such lists of their copyright works as may be provided, and periodically updated, by any of the applicants; and
(d) all future versions of the Kazaa file-sharing system contain the said non-optional key word filter technology; and
(e) maximum pressure is placed on existing users, by the use of dialogue boxes on the Kazaa website, to upgrade their existing Kazaa software program to a new version of the program containing the said non-optional key word filter technology; or

(ii) that the TopSearch component of the Kazaa system will provide, in answer to a request for a work identified in any such list, search results that are limited to licensed works and warnings against copyright infringement and that will exclude provision of a copy of any such identified work.

6. The operation of order 4 be stayed for a period of two months from today's date, or for such extended period as a judge may, on application, allow.

7. The applicants' claims for pecuniary relief against the infringing respondents be reserved for

determination at a hearing to be fixed on application for that purpose.

8. There be liberty to all parties to apply, on seven days notice:

(a) within a period of one month from today's date, in respect of the form of order 4 or 5;
(b) generally, in respect of any Court approval required for the purposes of order 5, or any order required for purposes related to order 6 or order 7.

9. The applicants' claims under the *Trade Practices Act 1974* (Cth), the *Fair Trading Act 1987* (NSW) and in respect of the tort of conspiracy all be dismissed.

10. The infringing respondents pay 90% of the costs incurred by the applicants to date in relation to this proceeding.

11. The proceeding be wholly dismissed as against the following four respondents ('the dismissed respondents'): Sharman License Holdings Ltd, Philip Morle, Brilliant Digital Entertainment Pty Ltd and Anthony Rose.

13. The applicants pay the costs incurred in relation to this proceeding by each of the dismissed respondents, provided that, in the case of those dismissed respondents who were represented at the trial jointly with infringing respondents, such costs shall be limited to costs other than those that would have been incurred, in any event, in connection with representation of the relevant infringing respondents.

Note: Settlement and entry of orders is dealt with in Order 36 of the Federal Court Rules.

SCHEDULE

No	Recording	Artist	Copyright Owner
1.	Passenger	Powderfinger	Universal Music Australia Pty Ltd
2.	My Happiness	Powderfinger	Universal Music Australia Pty Ltd
3.	Love Your Way	Powderfinger	Universal Music Australia Pty Ltd
4.	On My Mind	Powderfinger	Universal Music Australia Pty Ltd
5.	Rockin' Rocks	Powderfinger	Universal Music Australia Pty Ltd
6.	Sunsets	Powderfinger	Universal Music Australia Pty Ltd
7.	Here Without You	3 Doors Down	UMG Recordings, Inc.
8.	Lose Yourself	Eminem	Shady Records, Inc. /Interscope Records
9.	Superman	Eminem	Aftermath Records
10.	Clap Back	Ja Rule	UMG Recordings, Inc.
11.	It Wasn't Me	Shaggy	UMG Recordings, Inc.
12.	No need to argue	The Cranberries	UMG Recordings, Inc.
13.	Ode to my family	The Cranberries	UMG Recordings, Inc.
14.	Zombie	The Cranberries	UMG Recordings, Inc.
15.	Daffodil's Lament	The Cranberries	UMG Recordings, Inc.
16.	Empty	The Cranberries	UMG Recordings, Inc.
17.	Linger	The Cranberries	UMG Recordings, Inc.
18.	Talk About Love	Christine Anu	Mushroom Records Pty Ltd
19.	Island Home	Christine Anu	Mushroom Records Pty Ltd
20.	Breathe In Now	George	Mushroom Records Pty Ltd
21.	Coming Home	Alex Lloyd	EMI Music Australia Pty Ltd
22.	Rollover DJ	Jet	Real Horrorshow Pty Ltd
23.	Maitland Street	The Living End	The Living End Pty Ltd
24.	Tabloid Magazine	The Living End	The Living End Pty Ltd
25.	Come To This	The Sleepy Jackson	EMI Music Australia Pty Ltd
26.	Steal my kisses	Ben Harper	Virgin Records America, Inc.
27.	Please Bleed	Ben Harper	Virgin Records America, Inc.
28.	The Woman In You	Ben Harper	Virgin Records America, Inc.
29.	Clocks	Coldplay	EMI Records Ltd
30.	God Put a Smile Upon Your Face	Coldplay	EMI Records Ltd
31.	The Scientist	Coldplay	EMI Records Ltd

32.	Don't Panic	Coldplay	EMI Records Ltd
33.	Shiver	Coldplay	EMI Records Ltd
34.	Yellow	Coldplay	EMI Records Ltd
35.	Don't Dream It's Over	Crowded House	Capitol Records, Inc.
36.	Milkshake	Kelis	Arista Records, LLC
37.	Teardrop	Massive Attack ft. Tricky	Circa Records Ltd
38.	Come Away With Me	Norah Jones	Capitol Records, Inc.
39.	Seven Years	Norah Jones	Capitol Records, Inc.
40.	The nearness of you	Norah Jones	Capitol Records, Inc.
41.	Don't know why	Norah Jones	Capitol Records, Inc.
42.	Paranoid Android	Radiohead	EMI Records Ltd
43.	Karma Police	Radiohead	EMI Records Ltd
44.	Creep	Radiohead	EMI Records Ltd
45.	Kids	Robbie Williams	Chrysalis Records Ltd
46.	Sergeant Pepper's Lonely Hearts Club Band	The Beatles	EMI Records Ltd
47.	Son of a Gun	Janet Jackson	Virgin Records America, Inc.
48.	Innocent Eyes	Delta Goodrem	Sony Music (Australia) Pty Ltd
49.	Predictable	Delta Goodrem	Sony Music (Australia) Pty Ltd
50.	Animal	Jebediah	Sony Music (Australia) Pty Ltd
51.	Benedict	Jebediah	Sony Music (Australia) Pty Ltd
52.	Harpoon	Jebediah	Sony Music (Australia) Pty Ltd
53.	Ana’s Song (Open Fire)	Silverchair	Sony Music (Australia) Pty Ltd
54.	Feeler	Pete Murray	Sony Music (Australia) Pty
55.	Freedom	Pete Murray	Sony Music (Australia) Pty Ltd
56.	Down Under	Men At Work	Sony Music (Australia) Pty Ltd
57.	I'm Alive	Celine Dion	Sony Music Entertainment (Canada), Inc.
58.	If You Had My Love	Jennifer Lopez	Sony BMG Music Entertainment
59.	Still	Jennifer Lopez	Sony BMG Music Entertainment
60.	My Stupid Mouth	John Mayer	Mayer Music LLC
61.	Better Man	Pearl Jam	Sony BMG Music Entertainment
62.	Daughter	Pearl Jam	Sony BMG Music Entertainment
63.	Elderly Woman Behind the Counter in a Small Town	Pearl Jam	Sony BMG Music Entertainment

64.	Immortality	Pearl Jam	Sony BMG Music Entertainment
65.	Fat Cop	Regurgitator	Warner Music Australia Pty Ltd
66.	Track 1	Regurgitator	Warner Music Australia Pty Ltd
67.	Blow Up The Pokies	The Whitlams	Timothy Freedman
68.	Thank You	The Whitlams	Timothy Freedman
69.	Breathing You In	The Whitlams	Timothy Freedman
70.	From the Inside	Linkin Park	Warner Bros. Records, Inc.
71.	Disease	Matchbox 20	Atlantic Recording Corporation
72.	When Doves Cry	Prince	Warner Bros. Records, Inc.
73.	Purple Rain	Prince	Warner Bros. Records, Inc.
74.	Meat Is Murder	The Smiths	Warner Music UK Ltd
75.	How Soon Is Now	The Smiths	Warner Music UK Ltd
76.	Winter	Tori Amos	Atlantic Recording Corporation
77.	Crucify	Tori Amos	Atlantic Recording Corporation
78.	The Music Box	Trans-Siberian Orchestra	Atlantic Recording Corporation
79.	Please Do Not Go	Violent Femmes	J. Ruby Productions, Inc. dba Slash Records
80.	By Myself	Linkin Park	Warner Bros. Records, Inc.
81.	In The End	Linkin Park	Warner Bros. Records, Inc.
82.	Music	Madonna	Warner Bros. Records, Inc.
83.	All I Need Is You	Guy Sebastian	BMG Australia Limited
84.	Just As I Am	Guy Sebastian	BMG Australia Limited
85.	What About Me	Shannon Noll	BMG Australia Limited
86.	Sk8er Boi	Avril Lavigne	Arista Records, LLC
87.	Toxic	Britney Spears	Zomba Recording LLC
88.	Fighter	Christina Aguilera	BMG Music (BMG Music dba The RCA Records Label, a Unit of BMG Entertainment)
89.	The Voice Within	Christina Aguilera	BMG Music (BMG Music dba The RCA Records Label, a Unit of BMG Entertainment)
90.	Thank You	Dido	BMG UK & Ireland Ltd
91.	White Flag	Dido	BMG UK & Ireland Ltd
92.	Don't Think Of Me	Dido	BMG UK & Ireland Ltd
93.	Here With Me	Dido	BMG UK & Ireland Ltd
94.	Honestly Ok	Dido	BMG UK & Ireland Ltd

95.	My Life	Dido	BMG UK & Ireland Ltd
96.	Slide	Dido	BMG UK & Ireland Ltd
97.	The Way You Move	Outkast	LaFace Records
98.	Trouble	Pink	LaFace Records

IN THE FEDERAL COURT OF AUSTRALIA
NEW SOUTH WALES DISTRICT REGISTRY **NSD 110 OF 2004**

BETWEEN: **UNIVERSAL MUSIC AUSTRALIA PTY LTD**
FIRST APPLICANT

FESTIVAL RECORDS PTY LTD AND MUSHROOM RECORDS PTY LTD TRADING AS FESTIVAL MUSHROOM RECORDS
SECOND APPLICANT

EMI MUSIC AUSTRALIA PTY LIMITED
THIRD APPLICANT

SONY MUSIC ENTERTAINMENT (AUSTRALIA) LIMITED
FOURTH APPLICANT

WARNER MUSIC AUSTRALIA PTY LIMITED
FIFTH APPLICANT

BMG AUSTRALIA LIMITED
SIXTH APPLICANT

UMG RECORDS, INC.
SEVENTH APPLICANT

SHADY RECORDS, INC./INTERSCOPE RECORDS
EIGHTH APPLICANT

AFTERMATH RECORDS
NINTH APPLICANT

REAL HORRORSHOW PTY LTD
TENTH APPLICANT

THE LIVING END PTY LTD
ELEVENTH APPLICANT

VIRGIN RECORDS AMERICA, INC.
TWELFTH APPLICANT

EMI RECORDS LTD
THIRTEENTH APPLICANT

CAPITOL RECORDS, INC
FOURTEENTH APPLICANT

ARISTA RECORDS, LLC (FORMERLY KNOWN AS ARISTA RECORDS, INC.)
FIFTEENTH APPLICANT

CIRCA RECORDS LTD
SIXTEENTH APPLICANT

CHRYSALIS RECORDS LTD
SEVENTEENTH APPLICANT

SONY MUSIC (AUSTRALIA) PTY LTD
EIGHTEENTH APPLICANT

SONY MUSIC ENTERTAINMENT (CANADA) INC.
NINETEENTH APPLICANT

SONY BMG MUSIC ENTERTAINMENT
TWENTIETH APPLICANT

MAYER MUSIC LLC
TWENTY-FIRST APPLICANT

TIMOTHY JAMES FREEDMAN
TWENTY-SECOND APPLICANT

WARNER BROS. RECORDS, INC.
TWENTY-THIRD APPLICANT

ATLANTIC RECORDING CORPORATION
TWENTY-FOURTH APPLICANT

WARNER MUSIC UK LTD
TWENTY-FIFTH APPLICANT

J RUBY PRODUCTIONS, INC. DBA SLASH RECORDS
TWENTY-SIXTH APPLICANT

ZOMBA RECORDING LLC (FORMERLY KNOWN AS ZOMBA RECORDING CORPORATION)
TWENTY-SEVENTH APPLICANT

BMG MUSIC (BMG MUSIC DBA THE RCA RECORDS LABEL, A UNIT OF BMG ENTERTAINMENT)
TWENTY-EIGHTH APPLICANT

BMG UK & IRELAND LTD
TWENTY-NINTH APPLICANT

LAFACE RECORDS
THIRTIETH APPLICANT

AND: **SHARMAN LICENSE HOLDINGS LTD**
FIRST RESPONDENT

SHARMAN NETWORKS LTD
SECOND RESPONDENT

LEF INTERACTIVE PTY LTD
THIRD RESPONDENT

NICOLA ANNE HEMMING
FOURTH RESPONDENT

PHILIP MORLE
FIFTH RESPONDENT

ALTNET INC
SIXTH RESPONDENT

BRILLIANT DIGITAL ENTERTAINMENT INC
SEVENTH RESPONDENT

BRILLIANT DIGITAL ENTERTAINMENT PTY LTD
EIGHTH RESPONDENT

KEVIN GLEN BERMEISTER
NINTH RESPONDENT

ANTHONY ROSE
TENTH RESPONDENT

JUDGE: **WILCOX J**
DATE: **5 SEPTEMBER 2005**
PLACE: **SYDNEY**

REASONS FOR JUDGMENT

WILCOX J:

1 This proceeding raises important issues about Internet file-sharing.

2 My reasons are structured as follows:

I THE LITIGATION
(i) The parties paras 3 to 11
(ii) The proceeding paras 12 to 21
(iii) The trial paras 22 to 30

II THE PARTIES' POSITIONS
(i) The applicants' claims paras 31 to 51
(ii) The Sharman respondents paras 52 to 53
(iii) Mr Morle paras 54
(iv) The Altnet respondents paras 55 to 56
(v) Mr Rose paras 57

III THE KAZAA SYSTEM
(i) Electronic sound recordings paras 58
(ii) Description of Kazaa system paras 59 to 66

(iii) A user's perspective
(a) The Kazaa website paras 67 to 71
(b) KMD v2.6 paras 72 to 84
(c) Kazaa Plus v2.6 para 85
(d) KMD of v3.0 and Kazaa Plus v3.0 paras 86 to 87
(e) The End User Licence Agreement paras 88 to 91
(f) The 'Sharman team' paras 92 to 93
(iv) Sharman and the Kazaa System
(a) Control of Sharman paras 94 to 99
(b) The Sharman-Kazaa agreements paras 100 to 101
(c) The Sharman-Joltid agreements paras 102 to 106
(d) The Sharman-Altnet relationship paras 107 to 128

(v) The technical experts' agreed propositions para 129

(vi) The relationship between gold and blue files paras 130 to 135

IV MAJOR FACTUAL ISSUES IN THE CASE

(i) Knowledge and intention

(a) Documentary evidence paras 136 to 162

(b) Mr Morle's evidence paras 163 to 180

(c) Conclusions about knowledge and intention paras 181 to 194

(ii) Technological controls

(a) Direct control through a

central server paras 195 to 235
(b) The range of indirect controls paras 236
(c) Monitoring of Kazaa users' files paras 237 to 244
(d) User identification system paras 245 to 249
(e) Termination paras 250 to 253
(f) Keyword filtering paras 254 to 294
(g) 'Persuaded' upgrades paras 295 to 309
(h) Gold file flood filter paras 310 to 330

(iii) Non-technological controls
(a) Warnings paras 331 to 340
(b) Enforcement by legal action paras 341 to 351

V THE AUTHORISATION ISSUE
(i) The statutory provisions paras 352 to 362
(ii) Submissions of counsel paras 363 to 394
(iii) The application of s 112E paras 395 to 399
(iv) The application of s 101 to Sharman and Sharman Holdings paras 400 to 420
(v) The application of s 101 to LEF and Ms Hemming paras 421 to 447

(vii) The application of s 101 to Mr Morle paras 448 to 451
(viii) The application of s 101 to the Altnet companies paras 452 to 473

(viii) The application of s 101 to Mr Bermeister paras 474 to 479
(ix) The application of s 101 to Mr Rose paras 480 to 488
(x) Conclusions on authorisation paras 489 to 490

VI THE TRADE PRACTICES CLAIMS

(i) Misleading conduct paras 491 to 502
(ii) Unconscionable conduct paras 503 to 509

VII THE CONSPIRACY CLAIMS paras 510 to 516
VIII DISPOSITION paras 517 to 526

I THE LITIGATION

(i) The parties

3 There are 30 applicants in the proceeding. The first to sixth applicants commenced the proceeding. Those applicants are all Australian companies, although most (if not all) of them are substantially owned and controlled by overseas parent companies. Those six applicants distribute sound recordings in Australia. They claim copyright in their respective sound recordings pursuant to the *Copyright Act 1968* (Cth) ('the Act'). I will refer to these six applicants as 'the original applicants'.

4 The 7th to 30th applicants were added by amendment of the Application. Most of these applicants are companies incorporated outside Australia, although two are Australian companies and one is a natural person. These 24 applicants also claim copyright in sound recordings.

5 There are ten respondents. The first five respondents were original parties. The second five respondents were added as parties following the execution of *Anton Pillar* orders made by me on the day the proceeding was commenced.

6 It is convenient to divide the ten respondents into four groups, reflecting their representation at the trial.

7 The first group (the first to fourth respondents) consists of three companies, Sharman License Holdings Ltd ('Sharman Holdings'), Sharman Networks Ltd ('Sharman'), LEF Interactive Pty Ltd ('LEF') and one natural person, Nicole Anne Hemming ('Ms Hemming'). Sharman Holdings and Sharman ('the Sharman companies') were both incorporated in Vanuatu. LEF is an Australian company. The sole director and shareholder of LEF is Ms Hemming. She is also the Chief Executive Officer ('CEO') of Sharman. Ms Hemming is not a director of that company or of Sharman Holdings. Consistently with the course taken at trial, I will refer to the three companies and Ms Hemming, collectively, as 'the Sharman respondents'.

8 The fifth respondent, Philip Morle, was at material times Director of Technology of LEF. His services were made available to Sharman, apparently on a full-time basis. His responsibilities at Sharman were consistent with him having been Director of Technology of Sharman itself. I will regard him as having filled that position.

9 The first to fifth respondents have sometimes collectively been called the 'Sharman parties'. They have also been referred to as the 'Kazaa parties', on account of the fact that, with the possible exception of Sharman Holdings, they are all concerned with the operation of the Kazaa computer software system which lies at the heart of this case.

10 The third group (the sixth to ninth respondents) also consists of three companies and one natural person. The three companies are Altnet Inc ('Altnet') and Brilliant Digital Entertainment Inc ('BDE'), both American companies, and Brilliant Digital Entertainment Pty Ltd ('BDE Pty Ltd'), an Australian company. I will call these three companies 'the Altnet companies'. The natural person is Kevin Glen Bermeister ('Mr Bermeister'), a person who has a significant role in the affairs of all the Altnet companies. I will refer to the Altnet companies and Mr Bermeister, collectively, as 'the Altnet respondents'.

11 The tenth respondent is Anthony Rose, a person who is said to be Chief Technical Officer of BDE. I will refer to the Altnet respondents and Mr Rose, collectively, as the 'Altnet parties'.

(ii) The proceeding

12 The proceeding was commenced on 5 February 2004. On that day, I made *Anton Pillar* orders authorising

representatives of the applicants and their solicitors, not more than two identified 'forensic experts' and one identified 'independent solicitor', to enter and search various premises apparently occupied by one or more of the Kazaa parties. I also made orders authorising such people to enter and search the premises of three identified universities. These universities were referred to as 'supernode parties', on account of an allegation that each of their computers was being used as a 'supernode' in Internet file sharing. The applicants did not claim the universities were knowingly involved in wrongdoing and did not join them as respondents in the proceeding.

13 The orders made on 5 February 2004 were executed. They were subsequently amended. It is unnecessary to refer to the detail of either the execution or the amendments. It is sufficient to say that, as a result of execution of the orders, the applicants took possession of a quantity of electronic data, most of which was provided in computer disc ('CD') form.

14 Between the institution of the proceeding and the commencement of the trial, on 29 November 2004, numerous interlocutory applications were made. I need not mention them all. However, I note three important interlocutory orders.

15 On 23 March 2004, I directed that '[a]ll issues of the quantum of pecuniary relief be determined separately from and after all other issues' and, unless otherwise ordered, interlocutory steps be confined to the other issues; that is, interlocutory steps were not to be taken in relation to the issue of the quantum of pecuniary relief (damages or an account of profits). It was on that day that I granted leave to the applicants to serve an Amended Application adding the Altnet parties to the proceeding.

16 On 14 September 2004, as a result of argument in connection with one interlocutory application, the applicants obtained leave to add the 7th to 30th applicants. They also obtained leave to amend their Statement of Claim so as to confine their claims of past infringement of copyright to 98 specified sound recordings ('Defined Recordings') that were subsequently listed in Schedules A to F of the Amended Statement of Claim filed on 15 October 2004 ('the S of C'). The Schedules identify each claimed copyright owner.

17 There is uncontested evidence that each of the Defined Recordings has been able to be downloaded, and has been downloaded, through the file-sharing facility of the Kazaa system.

18 In limiting their claims to the Defined Recordings, the applicants did not concede the copyright infringements that had been allegedly committed by the respondents were confined to those recordings. The applicants' decision to limit their claims arose out of their logistical difficulty in establishing the copyright chain of title for each of the many sound recordings whose copyright the respondents are alleged to have infringed.

19 On 1 November 2004, I heard argument, pursuant to a notice of motion filed on 26 October 2004, concerning an application by three organisations for leave to intervene in the proceeding. The applicants for leave were Australian Consumers' Association Pty Ltd, Electronic Frontiers Australia Inc. and New South Wales Council for Civil Liberties Inc. ('the Amici'). The Amici expressed concern that the decision in this case might unduly constrain freedom of speech.

20 The application for intervention was opposed by the applicants in the principal proceeding but supported by all the respondents. On 1 November 2004, I did not finally dispose of the application for intervention. I considered it would be preferable to defer a decision on the application until consideration of final

submissions and having regard to the content of the submissions offered by the Amici. I indicated I would not be prepared to allow intervention to prolong the hearing of the matter or to increase significantly the costs burden of other parties; however, I would be prepared to receive and consider a submission at the end of the case that was relevant, and not repetitive of points made by other parties.

21 In due course, counsel for the Amici provided a written submission. The submission presents a number of difficulties, as counsel for the applicants have pointed out. In particular, the submission seeks to have the Court consider documentary material that is not in evidence. This course is not open to me. On the other hand, the submission makes some useful comments about the proper interpretation of the Act. I will grant leave to the Amici to intervene to the extent necessary for them to put submissions that do not depend on material not already in evidence. I have given consideration to their submissions and will refer to them later.

(iii) The trial

22 Sixty-one affidavits, many lengthy, made by 34 witnesses, were read at the trial. Seventeen of those witnesses also gave oral evidence. The taking of evidence was substantially completed on 17 December 2004. There remained some problems about documents. Those problems were addressed on 17 and 31 January 2005, following which counsel for all parties supplied written submissions that were discussed at a hearing on 22-23 March 2005. At the conclusion of that hearing, I reserved my decision.

23 An enormous quantity of evidence was tendered at the trial. Little of it was the subject of objection by other parties; probably correctly, as most of the material was not irrelevant to the wide issues raised by the pleadings and was not otherwise inadmissible. However, much of the material was unnecessary. There was considerable repetition, and over-elaboration, of evidence, even in relation to matters not seriously in dispute. Much of the material concerned peripheral matters that were never likely to be important.

24 Voluminous though it was, the evidence was also notable for what it lacked: direct evidence from those responsible for establishing and operating the Kazaa system, with its adjunct Altnet technology. Between them all, the respondents called only one witness who was directly involved in the operation of either the Kazaa or Altnet technology. That witness was Mr Morle. As Sharman's Director of Technology, he might have been expected to have a comprehensive knowledge of both the Kazaa and Altnet technology. However, he made a disappointing contribution to my knowledge of those matters. He claimed ignorance of many matters about which I would have expected him to be informed.

25 A further notable omission from the evidence was direct and definite identification of the Kazaa source code. Some expert witnesses examined what they thought to be a copy of the source code. Mr Morle gave evidence, under cross-examination by counsel for the Sharman parties, that he had instructed another person to send a library copy of what was thought to be the source code to Professor Keith Ross, one of the Sharman respondents' expert witnesses. However, neither Mr Morle nor anyone else confirmed the identity of the code perused by Professor Ross. Uncertainty about the content of Kazaa's source code complicated the hearing.

26 The principal parties relied heavily on evidence from so-called 'independent experts'. Much of this evidence was helpful, some of it extremely valuable. Some of this evidence was not helpful, either because it related to a peripheral, even irrelevant, matter or because I was compelled to form an adverse view about the objectivity or intellectual integrity of the witness. I mention, in this context, particularly Dr Roger Clarke, whose evidence on behalf of the Altnet parties was little more than a partisan polemic, and, to a lesser extent, Professor Ross.

27 As my task is to decide a lawsuit, rather than to write a book about the trial, I do not propose to summarise, or even mention, all the evidence. During the course of the trial, I paid close attention to all the evidence that was tendered, whether documentary, affidavit or oral. I have revisited most of that evidence in considering my decision and in formulating these reasons. However, I propose to refer only to those portions of the evidence that bear on the issues I need to decide, being guided in my selection by counsel's submissions.

28 These submissions were generally helpful. However, they are lengthy. Excluding supplementary material, they total 649 pages. Although I have read and reread them all, I will not attempt to respond to every point they raise.

29 From time to time, before and during the trial of this proceeding, reference was made to a proceeding then making its way through the United States courts. On 25 April 2003, the Federal District Court in Los Angeles summarily dismissed an action brought by various copyright holders against corporations allegedly associated with two United States-based peer-to-peer file-sharing systems, 'Grokster' and 'StreamCast'. The Court of Appeals for the Ninth Circuit affirmed that decision. However, after I had reserved judgment in this case, the United States Supreme Court unanimously reversed the lower courts and allowed the suit to go to trial. On 27 June 2005, the judgment was delivered: see *Metro-Goldwyn-Mayer Studios Inc v Grokster Ltd* 125 S.Ct 2764; 73 USLW 4675 *('Grokster')*.

30 It had always been obvious that there were similarities between the Kazaa system and the Grokster and StreamCast systems. There were also differences in the conduct of the systems' respective operators. Moreover, much of the Australian statutory law had no counterpart in United States law. So there was a question in my mind as to whether the Supreme Court's decision provided any guidance to the resolution of this case. On 30 June 2005, I invited the parties to comment about that matter. They all did so. Their comments confirmed my impression that the differences, both factual and legal, are such as to render *Grokster* of little assistance to me.

II THE PARTIES' POSITIONS

(i) The applicants' claims

31 Paragraphs 17 to 46 of the S of C relate to the subsistence and ownership of copyright. It is alleged that each of the original applicants controls a catalogue of 'sound recordings', within the meaning of the Act, which catalogue includes the sound recordings listed in a particular Schedule – that is, one of Schedules A to F – to the S of C. The S of C goes on to allege that the particular original applicant 'is exclusively licensed to make copies and authorise the making of copies in Australia' of those sound recordings in the relevant catalogue of which it is not the copyright owner.

32 Paragraphs 47 to 84 of the S of C make copyright claims against the Sharman companies. A cumulative and alternative claim is made against each company that it has, 'by itself or through or by its agents, developed, marketed and supplied to members of the public, including in Australia, certain computer software applications known as Kazaa Media Desktop ['KMD'] and Kazaa Plus' (collectively, 'the Kazaa Software').

33 By para 50 of the S of C, the applicants allege that each of the Sharman companies has, by itself or through or by its agents:

> *'(a) marketed the Kazaa Software to members of the public in Australia;*

(b) offered the Kazaa Software for download by members of the public in Australia;
(c) supplied the Kazaa Software to members of the public in Australia;
(d) developed and maintained and maintained [sic] *the Kazaa Software;*
(e) developed, maintained and made available technical features, resources and information required for the effective operation of the Kazaa Software, including the provision of indexes of supernodes;
(f) established, operated and maintained infrastructure used in the operation of the Kazaa Software or by users of the Kazaa Software, including multiple websites resolving to the URL www.kazaa.com;
(g) established, operated and maintained websites and services relating to the Kazaa Software located at the URLs www.kazaa.com, www.kazaaplus.com and www.sharmannetworks.com.'

34 Paragraph 51 of the S of C alleges that Kazaa Software has the following features and capabilities:

'(a) features that permit users of the Kazaa Software to search for, identify, locate and download MPEG-1 Audio Layer-3 (MP3) and other digital music files from other users of the Kazaa Software over the Internet;

(b) features that permit users of the Kazaa Software to make available MP3 and other digital music files for searching, identification, location and downloading by other users of the Kazaa Software over the Internet;

(c) the ability to designate the computers of certain users of the Kazaa Software as supernodes;

(d) features that permit the easy handling of MP3 and other digital music files by users of the Kazaa Software, including music specific searches, playlists and an inbuilt music player;

(e) features designed to encourage end users of the Kazaa Software to make available files and reward to them according to the number of files made available by them relative to the number of files downloaded by them from other users of the Kazaa Software, including the "Participation Level";

(f) features that permit users of the Kazaa Software to search for, identify and download digitally rights managed files, including music files, from or via Altnet or through or by its agents;

(g) the features and capabilities of the Altnet Technology pleaded in paragraph 97 below.'

35 The S of C goes on, in para 52, to claim that users of the Kazaa Software ('Kazaa Users') have, by means of that software:

'(a) made available for download by other users of the Kazaa Software;

(b) searched for and located, on the computers of other users of the Kazaa Software;
(c) downloaded from other users of the Kazaa Software; and
(d) thereby made copies of,

MP3 or other digital music files constituting copies of the whole or a substantial part of' the recordings over which the applicants claim rights as owners or licensees of the copyright.

36 Para 54 of the S of C contains an allegation that each of the Sharman companies did the acts complained of 'knowing and intending that, or being recklessly indifferent as to whether ... Kazaa Users would do the acts pleaded in' para 52 of the S of C.

37 The S of C proceeds to claim five different types of infringement:

(i) infringement by communication; that is, making available online, or electronically transmitting, to the public MP3, or other digital music file, constituting copies of the whole or a substantial part of the relevant sound recordings;
(ii) infringement by authorisation; that is, authorising Kazaa users to make available online, or electronically transmit, to the public MP3 or other digital music files constituting copies of the whole or a substantial part of the relevant sound recordings;
(iii) infringement by authorisation of the acts of each other Sharman company;
(iv) infringement by exhibition or distribution; that is, each of the file-shared sound recordings is an infringing copy of the relevant applicant's sound recording that is distributed by one or more of the Sharman companies; common design between those companies being alleged; and

(v) infringement as joint tortfeasors with Kazaa users.

38 The applicants pleaded that the file-sharing actions of Kazaa users were done without the licence of the relevant applicant. They alleged common design between each of the Sharman companies and Kazaa users and that the acts of the Sharman companies were done without the licence of the relevant applicant.

39 By paras 85 to 92 of the S of C, the applicants allege that Ms Hemming and Mr Morle authorised the acts of each of the Sharman companies and entered into a common design with them in respect of those acts.

40 Paragraphs 93 to 120 of the S of C make copyright claims against the Altnet companies. It is pleaded that each company, by itself or through or by its agents, 'developed, marketed and supplied for use in the Kazaa Software certain computer software technology (the Altnet Technology)'. Paragraph 96 alleges that each of the Altnet companies developed and designed the Altnet Technology 'in such a manner as to work in a complementary way with and form part of the Kazaa Software', and licensed that technology to Sharman and supplied it (and maintained it as part of the Kazaa Software) to members of the public in Australia. In particular, it is said each Altnet company 'established, operated and maintained infrastructure' that included 'computer servers from which Gold files are supplied to members of the public using the Kazaa Software'. Features and capabilities of the Altnet Technology are pleaded in para 97 of the S of C.

41 Paragraph 98 alleges that the infringing acts of Kazaa users 'were enabled or facilitated' by the Altnet

Technology and the pleaded acts of the Altnet companies.

42 The S of C goes to make infringement claims of the same five types as were earlier made against each of the Sharman respondents.

43 It is convenient immediately to note that, although the parties put some submissions about infringement types (i), (iv) and (v), the only types of infringement that are seriously arguable, having regard to the evidence, are (ii) and (iii). Realistically speaking, the applicants' copyright infringement claim depends entirely on the question whether the respondents, individually and/or jointly, authorised Kazaa users to infringe the applicant's copyright.

44 Paragraphs 121 to 128 of the S of C make claims against each of Mr Bermeister and Mr Rose that correspond, in relation to the Altnet companies, to those made against Ms Hemming and Mr Morle in relation to the Sharman companies.

45 Paragraphs 129 and 130 of the S of C contain allegations of accessorial liability (both authorisation and common design) each way, as between each Sharman party and each Altnet party.

46 Paragraphs 131 to 138 of the S of C contain allegations relevant to relief, including claims of flagrancy, knowledge and reckless disregard of copyright. These allegations were apparently intended to enliven s 115(4) of the Act.

47 Paragraphs 139 to 144 of the S of C claim that each of the Sharman companies made representations that were false and that constituted misleading or deceptive conduct, in contravention of s 52 of the *Trade Practices Act 1974* (Cth) ('the TP Act') and s 42 of the *Fair Trading Act 1987* (NSW) ('the FT Act'). Ms Hemming, Mr Morle and Mr Bermeister are said to have aided and abetted, or been knowingly concerned, in the contraventions.

48 The particular false representations claimed by the applicants against each of the Sharman companies are:

> *'(a) that it is not possible for them* [the Sharman companies] *to exercise control over the nature, quality or content of files that can be made available for download or downloaded by users via the Kazaa Software;*
>
> *(b) that it is not possible to exercise central control over the nature, quality or content of files that can be made available for download or downloaded by users via the Kazaa Software;*
>
> *(c) that a significant or substantial portion of the revenue generated via the Kazaa Software comes from payment for distribution of rights managed content;*
>
> *(d) that all files containing rights management information appear as gold icons in version 2.6 of the Kazaa Software;*
>
> *(e) that the performance of a personal computer will not be, or is unlikely to be, noticeably affected by its functioning as a supernode for the purposes of the Kazaa Software;*

(f) that functioning as a supernode for the purposes of the Kazaa Software will not, or is unlikely to, increase the cost of operating a personal computer;

(g) that a user of the Kazaa Software may avoid liability by altering the file data or metadata relating to infringing files;

(h) that a significant or substantial portion of files made available for download or downloaded by users via the Kazaa Software are non-infringing files.'

49 The applicants also pleaded claims of unconscionable conduct (paras 145 to 148 of the S of C) and conspiracy (paras 151 to 158 of the S of C).

50 The applicants' Second Further Amended Application, filed on 15 October 2004, sets out the relief claimed by them at the trial. The applicants claim declarations of infringement of copyright by each of the respondents; a permanent injunction against each respondent in relation to each sound recording in each particular applicant's catalogue, including each of the 98 Defined Recordings; damages (including damages pursuant to s 115(4) of the Act and for conversion pursuant to s 116(1)) or , at the option of the applicants, an account of profits; and delivery up of infringing copies and devices. The permanent injunction is proposed to be one restraining the particular respondent, personally or by servants or agents from:

(a) making, or authorising the making of, a copy of any of the Defined Recordings;
(b) communicating or authorising the communication of the whole or a substantial part of any of the said sound recordings to the public; or
(c) distributing articles embodying the said sound recordings.

Declarations, injunctions and damages are also sought in relation to the alleged false representations, misleading conduct, unconscionable conduct and conspiracy.

51 In view of the direction for separate trial made on 23 March 2004 (para 15 above), the parties have not tendered evidence, or made submissions, concerning the quantum of pecuniary relief. However, they (rightly) devoted attention at trial, and in their submissions, to the question whether the Court ought to grant declaratory and/or injunctive relief and, if so, in what form.

(ii) The Sharman respondents

52 In their Closing Submissions, counsel for the Sharman respondents expressed their clients' position in this way:

The principal issue in the proceeding is whether by distributing the bundle of software known as [KMD], the Sharman Respondents "authorise" infringements of copyright which may take place if users of the KMD make available in Australia infringing sound recordings (by placing them in their My Shared Folder and permitting them to be shared) or download in Australia digital files of such recordings using that software.

The Sharman Respondents' position in relation to that issue, broadly stated, is as follows –

(a) the KMD includes a Graphical User Interface (GUI) which permits access to

the peer-to-peer (or P2P) network known as FastTrack. By doing so it enables users with the software to search for and download files in a digital format from other users of FastTrack;

(b) the KMD is capable of being used, and is used, to make available and download files which do not involve any infringement of the Applicants' or any one else's copyright;

(c) the software is content neutral and the Sharman Respondents do not and are unable to control either the files (whether video, music, text or otherwise) which users might make available by placing them in their My Shared Folder or the content which they search for and choose to download using the software;

(d) in the context of "authorisation" there is a critical distinction between giving a person the power to do an infringing act and purporting to grant a person the right to do that act.

It is the Sharman Respondents' case that whilst, by distributing the KMD, they confer on users of the software the ability to make available for download by other users any files in digital format, they do not authorise any infringing acts in circumstances where it is conceded that the KMD software is capable of being used to communicate or download non-infringing material and the evidence establishes that they have no control over the user's use of the distributed software.

It is not to the point that the Sharman Respondents distribute the KMD in circumstances where they are aware that it is being used to engage in copyright infringing activity. ... Nor is it to the point that the Sharman Respondents receive revenue as a result of the distribution of the KMD.'

53 After noting the principal copyright claims made against their clients by the applicants, counsel said their clients' position was:

'(a) they have not communicated any infringing sound recordings to the public by reason of the fact that users of the KMD have either made those recordings available online or electronically transmitted them;

(b) an MP3 or other digital music file is not an "article" to which s.103 applies and they have not, by distributing the KMD, distributed "articles" within the meaning of s.103 of the Act;

(c) they have not authorised any infringements of copyright by users of the KMD by reason of those users doing in Australia acts comprised in the copyright (by either making recordings available online or electronically transmitting them); and

(d) they are not joint tortfeasors and have not conspired to injure the Appellants' or to do so by "unlawful means".

(iii) Mr Morle

54 In Closing Submissions, counsel for Mr Morle noted that the infringement allegations against him 'are effectively the same as those of the Sharman companies'. Counsel went on:

> *'It is important to keep clearly in mind the claims actually made against Mr Morle because the applicants' written outline ... habitually makes submissions addressed to the conduct of the respondents' collectively. This has the consequences that:*
>
> > *(a) in particular respects an impression is created that broader claims are asserted against Mr Morle than are pleaded; and*
> >
> > *(b) all of the conduct of all of the respondents is treated as relevant to a determination of the claims against Mr Morle as though it was all his conduct.*
>
> *All the claims made against Mr Morle rest on the fact that since January 2002 he has been an employee of the third respondent ("LEF") which has provided his services on a contract basis to the second respondent ("Sharman Networks"). Further they are all of an accessorial nature, save for the conspiracy claim.*
>
> *There is no principle (an inverse of the employer's vicarious liability for an employee's wrongs) which operates to make an employee responsible for the wrongs of his or her employer. Yet the unspoken assumption in the applicants' outline is that Mr Morle is to be treated as thus liable for any breaches of the Sharman companies, and by reason of their relationship with the Altnet companies, any breaches of the latter as well. No attention is given to specifically identifying facts from which it might be found that Mr Morle was an accessory of the companies in any instance.'*

(iv) The Altnet respondents

55 The Closing Submissions of counsel for the Altnet respondents commence with this statement in relation to the applicants' copyright claims:

> *'Irrespective of the Court's findings on issues of primary infringement by users and authorisation by Sharman, the principal case mounted against the [Altnet] respondents ... fails on the facts because the applicants have not shown that the Altnet Technology enables or* facilitates *any infringing conduct by users of [KMD]. To the contrary, the evidence points squarely to the conclusion that the Altnet Technology does* not *enable or facilitate any infringing acts, but instead is wholly directed to the provision of Gold Files. That finding, which is especially conspicuous by the contrary not being put by the applicants in their [Closing Submissions] is determinative of all copyright allegations made against the [Altnet] respondents.'*

56 Counsel put particular submissions concerning the other causes of action, to which I will return.

(v) Mr Rose

57 Counsel for Mr Rose adopted the submissions put by other respondents' counsel. They asserted these points 'apply with even greater force to Rose given his position in relation to the various corporate entities, and the fact that ... Rose is not a **significant figure** in the scheme of things' (original emphasis).

III THE KAZAA SYSTEM
(i) Electronic sound recordings

58 Before going to the Kazaa system itself, it may be useful for me to set out a slightly-edited general statement about electronic copying of sound recordings that was made at paras 131-136 of the Closing Submissions of counsel for the applicants. I believe this statement accords with the evidence and is uncontroversial.

> *'By the use of a computer installed with appropriate copying software, it is possible to create a high-quality "digital copy" of a sound recording embedded in a CD. This process is often referred to as "ripping" a CD. Such a process results in the production of a digital file or computer file. The digital file can be "played" on the computer which created the digital file using software which recognises such a file and uses it to generate audible sound. It can be transferred to a recordable CD and played in other equipment which recognises such files. It can be transferred to equipment which recognises and plays such files. It can be transferred over the Internet to other computers. Using appropriate software, the file can be converted to an audio file, transferred to a CD and played in an ordinary audio CD system.*
>
> *Different copying software produces computer files in different "formats". For example, a readily-available program is Windows Media Player. That enables a person to insert a commercially-released audio ... into the disc drive of a computer and create on the computer a digital copy of that sound recording in ".mp3" format.*
>
> *The mp3 format is a compressed format. The advantage of that format is that it constitutes a smaller computer file than a copy of the sound recording in an uncompressed format. The smaller computer file occupies less space on a computer drive and takes less time to transfer over the Internet. An mp3 file can be played in an mp3 player or on a computer. It can be downloaded over the Internet. It can be converted to an uncompressed audio file and burned onto a CD and played in an ordinary audio CD player. The ease by which this copying takes place is one of the causes of the problem of widespread infringement faced by the Applicants with the growth of file swapping. It is not, however, a basis to look favourably on the Respondents' exploitation of file swapping.*
>
> *It is possible to apply digitally rights managed technology ("DRM") to certain formats. One such format is the "WMA" format. DRM systems prevent the playing of a file except by a permitted user. For example, a user will normally require a unique licence number to play a file which may permit the playing of the file only on a particular computer. The mp3 format does not support DRM technology.*
>
> *There are legitimate Internet download music sites authorised by one or more of the Applicants. One example is "bigpondmusic.com" launched by Telstra on 15 January 2004. The legitimate music download services only make available digital copies of sound recordings with the DRM feature, usually in WMA format. They are not made available in mp3 format.*
>
> *The mp3 format is most commonly used for the creation and transfer of unauthorised copies of the Applicants' sound recordings. Virtually all of the acts of infringement of copyright in the Defined Recordings relates to mp3 copies of those recordings on the computers of Kazaa users.'*

(footnotes and headings omitted)

(ii) Description of the Kazaa system

59 The Closing Submissions of the Altnet respondents include a useful overview of the Kazaa system. The acronym 'KMD' refers to Kazaa Media Desktop, the free option of the program made available to users. The overview reads:

> *'(a) The KMD is a graphical user interface ("GUI") which permits access to two separate networks of computers connected to the internet: FastTrack and Joltid PeerEnabler, via means of which digital files including audio files may be transferred.*
>
> *(b) By means of FastTrack, KMD users can:*
>
> *i. Make available to other users files in their "My Shared Folder";*
> *ii. Search for files from other users in their "My Shared Folder";*
> *iii. Download such files from other users; and*
> *iv. Save such files in their My Shared Folder, in turn making them available to other KMD users.*
>
> *(c) The Joltid PeerEnabler network is quite different. First, Altnet controls all of the files which may be transferred on channels licensed by it – a user cannot choose to make available his or her own file (whether obtained lawfully or unlawfully) unless Altnet causes it to happen. Secondly, there is a list of files available on the PeerEnabler network resident on every participant's computer, from which it follows that there is no need to communicate with any supernode in order to respond to a search request. Thirdly, it is no part of the applicants' case that any of their copyright is infringed by the gold files distributed by Altnet through Joltid PeerEnabler.'*

60 The respondents claim the Kazaa system is an example of 'peer-to-peer' or 'P2P' technology. In their Closing Submissions, counsel for the applicants explained what that means:

> *'The name describes the capability of the software to enable the direct transfer of computer files between "peers" or individual computer users in a "network" in contradistinction to:*
>
> • *a system in which computer files are supplied from a single central computer to multiple individual computer users (eg, client/server), or*
>
> • *a system where even if files are not stored centrally, indexes are so stored...'*

61 Counsel for the applicants did not accept that Kazaa is truly a P2P system. They said that, 'while the software has P2P characteristics, it is now clear that it has many features in common with client/server and centrally indexed systems.'

62 At paras 178-201 of their Closing Submissions, counsel for the applicants set out a description of the

Kazaa system. Their description was supported by numerous references to the evidence given in this case. Whether or not the Kazaa system is truly P2P, most of this description is uncontroversial. Consequently, although it is lengthy, I will set it out, with only minor excisions, mostly to remove controversial comments. Footnote references have been omitted. Counsel said:

> *'The Kazaa system consists of millions of individual Kazaa users each having the Kazaa software installed on their own computers. Each such computer is referred to as a "node". A feature of the Kazaa system is that a small percentage of those computers (but still a large number in total) must function as "supernodes". A supernode computer must be a powerful computer with a fast Internet connection. There is an option available to a Kazaa user within the Kazaa software to ensure that his computer does not function as a supernode. It is to be inferred that ordinary users interfacing with the software at the basic operational level would not explore advanced functionality of that kind. Generally speaking, the software itself identifies potential supernode computers and causes them to function as supernodes. A Kazaa user is not told if his computer is being used as a supernode. However, as appears below, Sharman is able to force a computer to become a supernode.*
>
> *The Kazaa software is designed so that each supernode computer is connected (via the Internet) to a certain number of node computers. It appears that the number is between 100 and 200. A supernode is in constant communication with its nodes. Thus, each time a Kazaa user launches the Kazaa programme on his node computer (i.e., on the default option, on starting the computer), that computer will connect to and communicate with its supernode computer. Each supernode is connected to its nearest supernodes which in their turn are connected to other supernodes.*
>
> *A supernode is geographically proximate with its nodes.*
>
> *Once the Kazaa software is installed on a computer that is connected to the Internet, that computer forms part of a network or system consisting of all other computers connected to the Internet on which the Kazaa software is running. The user of that computer becomes a new Kazaa user. Every time the user connects to the Internet and launches the Kazaa program he is again connected up to the Kazaa system or network and to the Kazaa website.*
>
> *The Kazaa software creates a My Shared Folder on a user's computer upon installation of the software on the computer. The Kazaa software is designed so that the supernode computer operates to search the My Shared Folder of each of the ordinary nodes to which it is connected every 60 seconds. It assembles an index of all of the files in each of those My Shared Folders.*
>
> *The index contains the "metadata" and "filehash" of each file, along with the "IP Address" of the computer holding that file.*
>
> *"Metadata" is data associated with and which forms part of a file. It can include the name of the file such as the title of a sound recording, the name of the artist, a description of the quality of the file or the sound recording and the size of the file in bytes. The creator of the file or the recipient of the file can usually alter or add to metadata such as the name of the file and other descriptive material. However, "ripping" programs can typically access and automatically enter this information.*

A "filehash" is assigned by the Kazaa software to each file in a user's My Shared Folder based on the digital sequence of the file. It represents a shorthand version of the file which is the application of a mathematical algorithm to the longhand version of the file. The effect of it is to produce a short sequence of digits which, for all practical purposes, uniquely identifies that file. The same sound recording may be copied or "ripped" by different persons using different technologies to produce files which will sound the same when played but nevertheless will produce different filehashes due to idiosyncrasies in the different digital copying processes. Because the filehash is based on the content of the file, changing the name of the file - or in most circumstances the metadata - does not alter its filehash. The filehash of a file forms part of the file description included in the file indexing system. One benefit is that filehashing minimises the size of the index.

The "IP Address" or "Internet Protocol Address" is a unique number, akin to a telephone number, used by machines (usually computers) to refer to each other when sending information through the Internet using the Internet Protocol. This allows the machine passing the information onwards on behalf of the sender to know where to send it next, and for the machine receiving the information to know that it is the intended destination.

When an individual (ordinary node) Kazaa user types in a search term in the Search for Files box or in the appropriate box on the search page, that search request is sent to that computer's supernode. That communication is encoded and requires the relevant source code to be able to read the content of the communication. The supernode responds to the search request by reference to the index which it is constantly generating of all the files in the My Shared Folders of all of its connected nodes. The supernode may also forward the search request to other supernodes.

If the terms of a search request match any part of the metadata (eg artist name, or song title) of the files in the indices to which the search request is referred, those files are returned as matching Blue File search results to the user's computer as described above, distinguished by the blue Kazaa icon. Each matching result includes the title of the file, the name of the artist, the file size, an integrity rating and the username of the user in whose My Shared Folder the file is located ...

By clicking on the download icon next to the Blue File that represents a matching search result, the Kazaa software causes that file to be downloaded from the My Shared Folder of the Kazaa user where that file is located. A direct Internet link is established between the requesting user's computer and the supplying user's computer and the file is transferred via such direct link. The mechanism employed is to attach to each file in the search results the IP address of the computer holding that file. When the searching user clicks on the download icon for that file in the search results, the searching user's computer sends a request to that IP address for the file specifying the file by its filehash. The supplying user's computer responds by sending that file to the IP address of the searching user's computer, which IP address is provided with the request.

The Kazaa software also permits the simultaneous download of different parts of the same file from different sources in order to speed up the download process. In circumstances where the search result identifies files with the same filehash located in the My Shared Folders of different

Kazaa users, clicking on the download icon of the requested file sends requests for transfer to the different sources simultaneously. Different parts of the same file are supplied by different Kazaa users and are linked up to form a single file in the computer of the requesting user.

The direct transfer of files between users classifies the Kazaa system as a "peer-to-peer" network or system or "P2P". The description P2P is used to distinguish this method from a system which uses a central server or bank of servers to provide file content, although there is a difference between the Applicants and the Respondents about the extent to which the Kazaa system has server/client characteristics.

The supply by a Kazaa user of a file in his My Shared Folder to another Kazaa user requesting that file does not involve any additional act or step on the part of the supplying user. Once a file is in the supplying user's My Shared Folder and the user is online and with KMD running - the default option - is that the file can be the subject of a search result provided to another Kazaa user and a copy of that file can be transferred from the supplying user's My Shared Folder to the searching user's computer. ...

Files enter a Kazaa user's My Shared Folder in one of two ways. Firstly, a Kazaa user may transfer a file from another folder in his computer to his My Shared Folder or may cause a file being created by him or received by him from other sources to be saved in his My Shared Folder. For example, a Kazaa user who "rips" a sound recording to create an mp3 file might place that file in his My Shared Folder within the Kazaa programme in order that it can be "shared" with other Kazaa users.

Secondly, every time a Kazaa user downloads a file from another Kazaa user by clicking on the download icon next to a Blue File search result, a copy of the requested file is automatically transferred to the requesting user's My Shared Folder. Unless the requesting user takes the conscious step of removing the new file from his My Shared Folder to another folder in his computer, it is immediately available to be searched and downloaded by another Kazaa user. ... It is a design feature of the Kazaa software that downloads are automatically placed in a user's My Shared Folder. That has the tendency to maximise the number of files available to be shared on the system, which in turn makes it a more attractive system for putative file sharers to use. While a user can disable this feature, again, doing so is an advanced function that the ordinary user interfacing at the basic operational level is unlikely to select.

Files in the My Shared Folder of a Kazaa user cannot be searched and accessed by external users using search engines such as Google. They are not available to ordinary Internet users. Access to the files in the My Shared Folders of existing users is obtained by downloading and installing the Kazaa software. Those existing files are then available to the new Kazaa user. ...

Further, it is the capability of the Kazaa software to prepare indices of files in the My Shared Folders of Kazaa users, to match search requests by reference to those indices, to deliver the results of the search to a Kazaa user and to provide the mechanism for delivery of the requested file from one user to another, which makes the files available to users. The search results mechanism is a key aspect of the system. If a file does not appear in the search results, it is not available to be downloaded.

The Kazaa system or network may be described as a "distributed system". The system takes advantage of the resources of the computers owned or used by the individual Kazaa users. One obvious benefit of this is that the suppliers of the software do not have to supply the hardware or facilities on which the software and system is operated. A key benefit is that the files which users are interested in and searchable indices of those files can be located physically on a large number of different computers which are geographically spread around the world.

This has two advantages. First, it avoids the problem of a single computer or a single bank of computers having to deal with and respond to search requests and having to hold copies of all relevant files and respond to requests for those files. Such a centralized system may result in delays or a requirement of a large number of computers to be able to cope with the demand.

Secondly, the geographic spread of nodes and supernodes along with the design feature of the software of organising a supernode and its nodes in the same proximate geographical area has the consequence that the distance which most communications must travel is small and hence the response time is quick. ...

Hence the continuous addition of new Kazaa users to the system by the supply of the Kazaa software benefits both existing users and also makes the system more attractive for both existing and new users. As Mr Morle described it, every user gained adds value greater than one to the network and every user lost removes that value.

Equally, the more files of interest to other users that an individual user makes available in his My Shared Folder, the more attractive the system is likely to be to both existing and potential new users. The Kazaa software is designed so that Kazaa users are rewarded by participation levels based on the amount of files being uploaded from a user's My Shared Folder. The participation level of a user is automatically 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, and is displayed as a number and level name in the bottom left hand corner of the Kazaa software. A user who has a high participation level receives a greater priority from the Kazaa system over other users when attempting to download files. Therefore, a user who is sharing many popular files will be more easily able to download desired files.'

63 It will be noted, from the overview of the Kazaa system quoted at para 59 above, that it is the FastTrack technology that enables the file-sharing described in this extract.

64 There is evidence that the Kazaa blue files routinely include a high proportion of the most currently popular sound recordings. Anthony Ellis Johnsen, an employee of the Australian Recording Industry Association ('ARIA'), accessed KMD v2.7 one to three times per week in each of the weeks from 14 June 2004 to 13 September 2004. By reference to the artists' names and the titles of the recordings, he searched for files of the songs that appeared on ARIA's latest weekly lists of the top 50 or 100 singles recordings. Where he was able to do so, Mr Johnsen downloaded these files onto the hard drive of his computer and copied them onto DVD.

65 Mr Johnsen exhibited to his affidavit, dated 29 September 2004, documents setting out the results of two searches. On 14 June 2004, he found 34 of the Aria Top 50 singles in Kazaa blue files. On 21 June 2004, he found 85 of the Aria Top 100 singles. He was able to download all but a few of them.

66 Mr Johnsen's evidence was not challenged. He was not required to attend for cross-examination. It was not suggested his search results were atypical.

(iii) A user's perspective
(a) The Kazaa website

67 Any person with access to the Internet can become a Kazaa user. A person obtains access to the computer program through the Kazaa website (*http:/www.kazaa.com*). The website offers a choice of two programs: KMD, which is free to the user but contains advertisements; and Kazaa Plus, which requires payment of a once-only subscription of $US29.95 but is advertisement free.

68 At the commencement of this proceeding, the relevant versions of both these programs were numbered '2.6'. At that time, the Kazaa website prominently featured two banners. One was headed 'Kazaa v2.6', above the words:

> *'Free – Ad Supported*
>
> *- Search for and download files*
> *- Up to 24 Concurrent Searches*
> *- New Improved Interface*
> *- Download Now!'*

The other banner promoted Kazaa Plus v2.6, with a message ending 'Get it Now!'. Underneath the two banners were the words: 'The world's most downloaded software application! Over 2.4 million downloaded last week.'

69 The website also contained the following words, in smaller lettering:

> *'Kazaa is the World's Number 1 file sharing software application and it's available for free! Download it now to access the world of P2P (peer-to-peer). Search for and download music, documents, images, playlists, software, and videos. Play/View/music, image, software and video files. Distribute your original content with Kreate. Read more about Kazaa v2.6. Read The Guide. Learn about peer-to-peer (P2P). How is Kazaa free? Read more ... Sharman Networks Find out about the company that develops Kazaa software.'*

The underlined words provided click-on links to other webpages that provided additional information or guides to further action.

70 At the foot of each webpage, there appeared the following words in small print:

> *'Copyright: Sharman Networks Ltd does not condone activities and actions that breach the rights of copyright owners. As a Kazaa user you have agreed to abide by the End User License Agreement and it is your responsibility to obey all laws governing copyright in each country.'*

I will refer later to the terms of the End User Licence Agreement ('EULA').

71 The procedure, at that time, was that a person who wished to install either of the two programs had to enter a username and country and click 'Kazaa v2.6'. The user was then taken to a page that required a choice between 'Kazaa Plus v2.6' and 'Kazaa v2.6'. Under a heading 'What You Install With Kazaa v2.6

(free version)', the following material appeared:

> '[diamond] *Kazaa Media Desktop (KMD) – this is the main application that lets you search for, download and share files.*
> [diamond] *TopSearch – this displays quality, digitally rights managed files (marked with Gold icons) in search results. Powered by Altnet.*
> [diamond] *Altnet Peer Points Manager – this is a rewards application for sharing files marked with Gold icons. Includes My Search Toolbar, Joltid P2P Networking & Altnet Peer Points Components.*
> [diamond] *BullGuard P2P – BullGuard P2P provides virus protection when using Kazaa Media Desktop.*
> [diamond] *Advertising – delivered by Cydoor and the GAIN Network. Read more.*
> [diamond] *PerfectNav – Provides alternative websearch results when browsing.'*

(b) KMD v2.6

72 A person who selected the free program, KMD, was taken to a site, remote from the Kazaa website, called 'Kazaa Media Desktop 2.6 popular'. Amongst the items of information on this webpage, at the date of commencement of the proceeding, were the following:

> *'Downloads: 317,552,315*
>
> *Publisher: Sharman Networks Limited'*

73 The webpage also contained a 'Publisher's Description' that read:

> *'Kazaa Media Desktop is the world's No. 1, free, peer-to-peer, file-sharing software application. Features include improved privacy protection; the ability to search for and download music, playlists, software, video files, documents, and images; the ability to set up and manage music and video playlists; and the ability to perform multiple simultaneous searches, including up to five Search Mores, which deliver up to 1,000 results per search term.'*

74 The KMD Installer comprised a six-step process. Each of the different steps were displayed on the user's screen on a progressive basis. The first step contained this note:

> *'Welcome*
>
> *With Kazaa Media Desktop, you will be able to connect to the largest network of peers on the planet and:*
>
> *• Search for and download audio/music, documents, images, playlists, software, and video files.*
> *• Play or view audio/music, images and video files.*
> *• Share your original content with millions of users.*
> *• Access, trial and enjoy premium quality files.'*

75 Step two required the user to click a box reading:

> *'I agree to the Kazaa Media Desktop End User License Agreement and Altnet Peer Points Manager Package End User License Agreements.'*

Once again, the underlined material linked to other webpages.

76 Step four of the installer offered some options. There was a 'family filter, designed to block key adult and offensive terms'. The filter operated unless it was specifically discarded by the user. There was also an option to permit other users directly to browse the user's 'My Shared Folder' file, as distinct from searching the user's 'My Shared Folder' for an identified file. Permission depended upon the user making a deliberate choice to that effect.

77 Step five of the installer stated that installation of KMD enabled peer-to-peer ('P2P') networking and access to the Altnet system. Step six explained that P2P was 'connecting directly to other users via the Internet in order to communicate or share files'. The window contained this exhortation:

> *'**Sharing.** Responsible sharing is the cornerstone of a useful peer-to-peer experience. In order for everyone to benefit from the collaboration, users need to share appropriate files. Read more.'*

78 A 'P2P Networking' box stated:

> *'P2P Networking is a free component from Joltid Ltd and is part of Joltid(tm) PeerEnabler(tm)*
>
> *P2P Networking will give you*
>
> *· Access to a free P2P network*
> *· Content verified by publishers*
> *· High speed downloads*
> *· Privacy and security*
>
> *Note that files downloaded with P2P Networking will be shared out to other P2P Networking users.'*

79 A website page headed 'Got a Favorite Tune?' explained the difference between gold and blue files. It said this:

> *'About Premium and Other Content*
>
> *Each file in your search results is marked with either a Gold or Blue icon*
>
> ***Gold***
> *Files marked with a Gold icon are high quality files bought to you from professional content creators via Altnet. All files marked with Gold icons are digitally rights managed and are typically offered for use either on a free basis, or on a free-trial basis, before the file must be paid for.*

Blue
A Blue icon identifies all other files found in users' shared folders.

Kazaa Media Desktop (KMD) uses peer-to-peer (P2P) technology. This means that individual users connect to each other directly, without need for a central point of management. All content found in KMD search results is shared either by our premium content providers via Altnet or by other KMD users.'

80 A webpage explained P2P:

'Kazaa uses peer-to-peer technology. This means that individual users connect to each other directly, without need for a central point of management.

All you need to do is install Kazaa and it will connect you to other Kazaa users.

For example Peter downloads Kazaa and installs it onto his computer. Mary also has Kazaa installed on her computer. Peter uses Kazaa to search for a file he is looking for. Kazaa finds the file on Mary's computer. Peter can now download the file directly from Mary. (Illustration omitted)

Kazaa allows you to:

• Search and download content that is shared by premium content providers (files marked with Gold Icons) or by other Kazaa users.
• Promote and distribute your own files using Kazaa and Magnet Links. Find out more in the "Make it" section.

The P2P searches occur through users with fast connections, called Supernodes. Once located, the file is sourced for downloading directly from the user who has it.'

81 The Kazaa v2.6 website provided a link to a site headed 'Join the Revolution'. It opened with these words:

*'**About the Revolution***
There is a revolution underway which is changing the world of entertainment. It will effect how you discover, buy and share songs, movies, games and ideas. Peer-to-peer technology is driving the revolution and it could make life better for everyone. Lower prices, unlimited catalogs and more.'

82 The site went on to extol the advantages of peer-to-peer distribution of data and to argue it was good for 'consumers, artists, producers and developers, labels production companies, libraries and owners and peer-to-peer companies.'

83 Under the heading 'Who's Trying to Stop It and Why?', these statements appeared:

'Kazaa and other peer-to-peer applications have been under attack from the major Record and

Movie companies and their industry bodies, the Recording Industry Association of America and Motion Picture Association of America. The Record and Movie companies are suing peer-to-peer software developers and the RIAA are suing peer-to-peer users.

This Revolution can benefit everybody. So why are they trying to stop it?

Copyright owners.

• These companies own the copyright to material that they sell. Some of them are afraid that peer-to-peer means everything is always available for free.
• Some of them don't believe that peer-to-peer users would pay a reasonable price for files.
• Since May 2002, peer-to-peer applications like Kazaa have offered copyright owners the ability to protect, promote and sell their works to millions of users. Everything is in place. They just need to try it.

Record and Movie Companies

• These companies make money out of developing copyrighted material, distributing it, promoting it and selling it.
• They are concerned that peer-to-peer will reduce their control over every step of this process. This is because peer-to-peer is a market driven by the people.
• They think they will make less money.
• They'll have to change some of their business practices to succeed in a peer-to-peer environment, but all things need to change. Peer-to-peer should not be stopped because of this. The benefits of the technology are great. There should be no reason to try to halt a revolution.
• If peer-to-peer provides a bigger market, lower costs and unlimited space in packaging music, videos and pictures and these companies tried it, they could make so much more.
• They need to stop fighting this technology and start working with it. We'll say it again. Since May 2002, peer-to-peer applications like Kazaa have offered record and movie companies the ability to protect, promote and sell their works to the millions of users. Everything is in place. They just need to try it.'

84 The site went on to describe a method of licensed file-sharing, and concluded with exhortations to viewers to lobby politicians and the media for change.

(c) Kazaa Plus v2.6

85 It is not necessary to describe the installation steps for Kazaa Plus v2.6. The procedure was similar to that for KMD v2.6, but with use of a different licence agreement.

(d) KMD v3.0 and Kazaa Plus v3.0

86 Kazaa v3.0 and Kazaa Plus v3.0 were made available to users about one week before trial of this proceeding commenced. A website page contained this suggestion: 'Search for and download music, movies, software, images and documents'. The webpage stated: 'Having Kazaa is 100% Legal'. On another website page, under the heading 'Responsible sharing with Kazaa', the following material appeared:

'You will have access to millions of peers around the world. You can publish your self-authored content. Just place public domain content and/or your photos, book, articles, art work or independent films in your "My Shared Folder" and users worldwide will be able to find and download them.

You can promote your blog or website to other users via Kazaa and find other users' blogs and sites.

Magnet Links allow you to super-distribute your talent ... your peers can promote your work via links! Magnet links allow web sites to link directly to files that can be downloaded with P2P technology. This can result in significant savings in online distribution and hosting costs.

If you want to make money by distributing content via Kazaa, contact Altnet. Altnet provides a Digital Rights Management solution which allows artists and content creators to distribute files securely on Kazaa, using free trial or pay-to-play/use licenses.

With peer-to-peer technology like Kazaa, individual users connect to each other directly, without a central point of management. All content found in Kazaa search results is shared either by premium content providers via Altnet, or by other Kazaa users. Sharman Networks Ltd, makers of Kazaa, does not condone activities and actions that infringe the rights of copyright owners. As a Kazaa user, you must agree to abide by the End User License Agreement and it is your responsibility to obey all laws governing copyright in each country.'

87 It is not necessary for me to describe the detail of the Kazaa v3.0 website material. It was similar to that on the Kazaa v2.6 website. The Kazaa v3.0 website contained a form of licence agreement governing sharing of works over which the user might hold copyright.

(e) The End User Licence Agreement

88 There is little difference between the KMD v2.6 and KMD v3.0 EULAs. Where there is a difference in the quoted material, I will show the difference in parenthesis.

89 The purported effect of both forms of agreement was that acceptance would create a licence agreement between Sharman and the user 'for the use of the Kazaa Media Desktop [Software], including any and all versions or variations' of that software and 'any future fixes, updates and upgrades provided to the user'. Clause 1.1 of the agreement contained a grant to the user by Sharman of 'a limited, non-exclusive, personal, non-sublicensable, non-assignable licence to install and use [the software] on a computer'. Clause 4.4 contained a note about the 'My Shared Folder' file:

'By saving a file in My Shared Folder, you understand that it will be available for any other user of Kazaa [Media Desktop] and compatible programs. These users may find your files and subsequently download them from you. By doing so your Internet connection is being used.'

The subclause went on to explain how to disable sharing.

90 Clause 4.5 referred to the possibility of the user's computer serving as a supernode. The subclause explained:

'Your copy of the Software may serve as a SuperNode. The selection process is automated. When your computer is a SuperNode other peers will upload an index of files they are sharing to your computer and they will send search queries to your computer. Your computer will reply to these requests and also forward the request to other SuperNodes.'

The subclause instructed the user what to do if he or she did not wish to serve as a supernode.

91 Clause 6 dealt with copyright infringement. It stated:

'6.1 Sharman respects copyright and other laws. Sharman requires all Kazaa [Media Desktop] users to comply with copyright and other laws. Sharman does not by the supply of the Software authorise you to infringe the copyright or other rights of third parties.

6.2 As a condition to use the Software, you agree that you must not use the Software to infringe the intellectual property or other rights of others, in any way. The unauthorised reproduction, distribution, modification, public display, communication to the public or public performance of copyrighted works is an infringement of copyright.

6.3 Users are entirely responsible for their conduct and for ensuring that it complies with all applicable copyright and data-protection laws. In the event a user fails to comply with laws regarding copyrights, [or] other intellectual property rights, [and] data-protection and privacy, such a user may be exposed to civil and criminal liability, including possible fines and jail time.'

(f) The 'Sharman team'

92 Both the Kazaa v2.6 website and the Kazaa v3.0 website contained information about Sharman. Under the heading 'Who are we anyway?', both websites stated:

'Kazaa.com, Kazaa Media Desktop and Kazaa Plus are products of Sharman Networks. Sharman Networks is a proactive, virtual, global technology and publishing company, focused on delivering peer-to-peer software.'

93 Under a heading 'Meet the Sharman Networks Team', there were photographs of Ms Hemming (described as 'CEO') and Mr Morle (described as 'Director of Technology'). There was also a photograph of Alan Morris, who was described as 'Vice President'.

(iv) Sharman and the Kazaa system
(a) Control of Sharman

94 Sharman was incorporated, in the Republic of Vanuatu, on 15 January 2002. Sharman Holdings was incorporated, also in Vanuatu, on 6 June 2003. There is no evidence before the Court as to why it was decided to incorporate those companies in that country. The evidence does not reveal any other connection between Vanuatu and any of the present parties or their activities. Perhaps the reason was that s 125 of the Vanuatuan *International Companies Act* makes it an offence, punishable by a fine of up to $100,000 or imprisonment for up to five years, for anybody to reveal, or to induce a person to reveal, information about the controllers of a Vanuatuan international company.

95 Notwithstanding this, answers to interrogatories made by Ms Hemming, and tendered by the applicants, reveal that both the Sharman companies are owned by Vanuatu International Trust Company Limited ('VITCO'), that the sole director of each of them is Worldwide Nominees Limited and that they are controlled by Geoff Gee (a director of Worldwide Nominees Limited) and Lindsay Barrett, a director of VITCO. Mr Gee and Mr Barrett are apparently Vanuatu accountants. They are probably acting on behalf of others. In the result, and despite the best endeavours of the applicants' legal representatives to penetrate the veil of secrecy, the identity of the ultimate owners of the Sharman companies remains a mystery. Counsel for the applicants suggested that the owner, or one of the owners, was Mr Bermeister. There is no evidence supportive of that conclusion.

96 It was common ground at the trial that Mr Bermeister introduced Ms Hemming to Kazaa BV. The detail of the introduction was recounted in an Answer to Interrogatories made by Ms Hemming, which, of course, was only admissible against her.

97 I will set out para 4 of the Notice to Answer Interrogatories served upon Ms Hemming and her response. In doing so, I mention that Ms Hemming had stated, in answer to interrogatory 3(i), that she had said in an interview 'that Kevin Bermeister introduced me to the opportunity' of acquiring the business of Kazaa BV. Paragraph 4 reads:

> '***4. If the answer to interrogatory 3(i) is yes:***
>
> > ***(i) state whether Mr Bermeister put the opportunity to Ms Hemming orally or in writing;***
> >
> > ***(ii) if Mr Bermeister put the opportunity to Ms Hemming orally, state:***
>
> ***A. the substance of any conversations;***
> ***B. the identity of any other person present during the conversations;***
> ***C. the location of the conversation(s); and***
> ***D. the date and time of the conversation(s).***
>
> ***If Mr Bermeister put the opportunity to Ms Hemming in writing;***
>
> ***A. identify all Documents containing the said writing;***
> ***B. state the substance of the said Documents;***
> ***C. state whether the said Documents still exist; and***
> ***D. if the said Documents do exist, identify the person(s) with possession of the said Documents.***
>
> *4. (i) Orally.*
>
> > *(ii) A. Kevin talked about the fact that Kazaa BV was looking to sell its assets. He explained the nature of the software which Kazaa BV owned and which Kazaa BV was looking to sell. He explained the manner in which the software and Peer to Peer worked. He suggested that my*

background in publishing consumer products and my experience and history of building new businesses meant that this was potentially a good opportunity for me. He explained that Altnet had an existing relationship in place with Kazaa BV which provided for the Altnet technology to be bundled alongside Kazaa and that Altnet would provide a marketing and secure distribution mechanism for copyright owners using DRM solutions. He offered to introduce me if I was interested in buying any assets. In a subsequent conversation I asked him to introduce me to Kazaa BV. There were no other persons present during the conversations.

4. (ii)(C) Sydney

4. (ii)(D) December 2001.'

Kazaa BV was a Netherlands corporation, previously known as Consumer Empowerment BV.

98 Ms Hemming went on to say 'there were no investors'. That statement suggests Ms Hemming is herself the owner of the Kazaa business (perhaps in conjunction with others). Presumably somebody put money into Sharman to enable it to purchase the business from Kazaa BV and to commence its own operations.

99 Whether or not Ms Hemming is an owner, she appears not to be a director of either Sharman or Sharman Holdings. Neither does she appear to be an employee of either company. As mentioned above, she is the sole director of, and shareholder in, LEF. This company was registered on 21 February 2002, about one month after the incorporation of Sharman, presumably with the intention that it would be the vehicle by which Ms Hemming made her services available to Sharman. Apparently that happened. Ms Hemming's services seem to be made available (apparently to Sharman, not Sharman Holdings) pursuant to an agreement between Sharman and LEF.

(b) The Sharman-Kazaa agreements

100 Shortly after its incorporation, Sharman entered into two agreements with Kazaa BV. One agreement was for the purchase by Sharman of a business conducted by Kazaa BV. The business was described as being 'the Vendor's business and trade of the provision of peer to peer Internet enabled software (which includes advertisement space which can be used to display advertising to users) directly via the Website to end users world-wide to enable searching for and downloading files from other users of the software'. The Sharman respondents put in evidence a technical document which suggests the earliest 'Kazaa.exe' file is dated 16 October 2000. Neither the origin nor accuracy of this document was established.

101 By cl 2.1 of the other agreement, Kazaa BV granted to Sharman a non-terminable (except under cl 6 of the agreement) world-wide licence of 'the Technology and Improvements'. The word 'Technology' was defined in cl 1.1 to refer to the 'Fasttrack' peer-to-peer stack software, the KMD software and other software programs. Clause 6 provided that the licence should be for a minimum period of one year, and to continue thereafter but with each party having certain termination rights.

(c) The Sharman - Joltid agreements

102 At about the same time, Sharman made an agreement with a Virgin Islands company, then known as Blastoise Limited and later as Joltid Limited ('Joltid'). By cl 1 of this agreement, Joltid granted to Sharman 'a non-exclusive, perpetual, irrevocable, transferable, worldwide license to use, and sublicense to SHARMAN's end users', Joltid's peer-to-peer technology.

103 A later agreement between Joltid and Sharman, apparently made in October or November 2002, but backdated to commence on 18 January 2002, superseded the earlier software licence agreement. In this agreement ('the Joltid Licence Agreement'), Joltid was described as being 'the proprietor or licensee of certain peer to peer file sharing technology', defined to include software currently known as 'Kazaa Lib' or 'FastTrack P2P Stack', including updates thereof. Clause 3.1 of this agreement contained a grant by Joltid to Sharman of 'a non-exclusive, irrevocable, perpetual, worldwide, royalty-free licence to use the P2P Software and to sub-license such P2P Software to its users'. Clause 3.2 contained a grant by Joltid to Sharman of the right to have the software modified, adapted, customised, supported and maintained by a particular authorised developer, an Estonian company known as Bluemoon Interactive ('Bluemoon').

104 Counsel for the applicants contended that 'Sharman has effective control over modifications to the KazaaLib/FastTrack software which is integrated in the Kazaa software'.

105 The Joltid Licence Agreement contained limited rights of termination. However, cl 10.2 provided that termination 'shall not affect any accrued rights or liabilities of any party'; in particular, it was not to 'affect the perpetual nature of any licences granted pursuant to this Agreement'. Further, cl 10.3 required Joltid, on termination, to 'co-operate in good faith with Sharman, its agents, suppliers and contractors to assist with the orderly continuation of the Sharman business and continued use of the P2P Software and Documentation'.

106 Counsel for the applicants commented:

> *'The effect of the agreement is to vest practical ownership of the software in Sharman. It is a licence in name only.'*

(d) The Sharman-Altnet relationship

107 Altnet and BDE are both Delaware corporations. BDE was incorporated in 1996. It is a public, listed company. It has apparently always operated out of premises in California. At material times, BDE seems to have had six to eight directors. Only two of them, Mr Bermeister and Mark Miller, have been located in Australia. It seems that, at all material times, Mr Bermeister has been President and CEO. However, the company's annual reports suggest he is not the principal shareholder in the company.

108 According to a report filed by BDE with the United States Securities and Exchange Commission ('SEC'), BDE formed Altnet in February 2002:

> *'to create a private, secure, peer-to-peer network utilizing existing, proven technology to leverage the processing, storage and distribution power of a peer-to-peer network comprised of tens of millions of users'*

109 Since its formation, Altnet has been jointly owned by BDE (majority shareholder) and Joltid. Mr Bermeister has always been the sole director of Altnet.

110 The evidence contains little information about BDE Pty Ltd. It seems to be common ground that this company was formed or acquired by BDE in about October 2002, that its directors are Mr Bermeister and Mr Miller and that it has premises in Surry Hills, Sydney. There is no evidence as to what activities it carries on, there or elsewhere.

111 At one time, BDE had a relationship with Kazaa BV, stemming from two agreements made on 2 October 2001. One agreement related to advertising material. By that agreement, Kazaa BV appointed BDE as 'the exclusive 3D interactive, with audio, rich media advertising format' for Kazaa BV's websites and software applications. The second agreement was called 'Technology Bundle License Agreement'. By that agreement, BDE granted to Kazaa BV a:

> *'non-exclusive, non-transferable, worldwide license to use, and sublicense to [Kazaa BV's] end users, [BDE's] b3d projector and required technology ... as a required install component in all current and future versions and releases of [Kazaa BV's] peer to peer ('P2P') technology platform currently available on the Internet known as the KaZaa Media Desktop and built upon the FastTrack P2P technology'.*

112 On 7 February 2002, Kazaa BV, BDE and Sharman signed an agreement whereby Kazaa BV (with the approval of BDE) assigned to Sharman all its rights and obligations under the Technology Bundle License Agreement.

113 On 23 June 2003, Altnet and Sharman entered into a joint enterprise agreement. The recitals to the agreement ('the joint enterprise agreement') included that Sharman 'was created with the intention of working jointly with Altnet to develop a business by which the power of peer-to-peer file sharing could be used to distribute copyright licensed content to profit', that the two companies 'have been sharing revenue derived from the joint use of Sharman's and Altnet's technology pursuant to an oral agreement'; and that their 'joint commercial goals ... could not be attained except through the use and contribution by each of their respective technologies to this joint enterprise'.

114 Clause 1.10 of the joint enterprise agreement used the term 'Index Search Results' to mean:

> *'search results that are provided by Altnet's and/or a third-party's centrally controlled, distributed, or other type of index in response to KMD Technology users' search queries, such as those provided by Altnet through its TopSearch function'.*

115 By cl 2.1 of the joint enterprise agreement, Sharman appointed Altnet:

> *'as the exclusive (even as to Sharman) representative of Sharman for the sale, license, and/or other commercial exploitation of Index Search Results displayed on or otherwise accessed using the Kazaa GUI [Graphic User Interface] in response to end user search requests conducted using the KMD Technology'.*

116 Under cl 2.4, Sharman granted to Altnet, during the term of the joint enterprise agreement, 'a worldwide, non-exclusive, limited, non-transferable license to use Sharman's Marks, including without limitation "Kazaa", in connection with the exploitation by Altnet of its other rights hereunder'. The word 'Marks' was defined (by cl 1.15) to mean 'trademarks, service marks, trade names, and logos.'

117 Clause 3 of the joint enterprise agreement dealt with delivery of Altnet search results. Altnet was given

the right to display Index Search Results in the Kazaa GUI in response to search requests by users of the KMD technology and to deliver media and other content to users from Altnet's servers or other sources. Altnet's Index Search Results were to be the top three search results in the Kazaa GUI and were also to be at a ratio of not less than one result for every four non-Altnet search results. The Index Search Results referred to in this agreement correspond with what have been called 'gold files'.

118 Under cl 4.8 of the joint enterprise agreement, Altnet was required:

> *'to create, safely maintain, and preserve all statistical records of the responses of users of the KMD Technology to the content located through Index Search Results displayed for TopSearch Keywords, including the statistical data on Conversion Rates, and other records pertaining to licensing the content located by Index Search Results by the users of the KMD Technology, in an understandable form, in the English language'.*

119 Clause 5.1 of the joint enterprise agreement provided for Sharman and Altnet to share net revenue in agreed proportions.

120 The joint enterprise agreement was terminable only for insolvency or material breach or (by Sharman) if gross revenue failed to reach an agreed baseline figure.

121 Counsel for the applicants contended that Sharman and the Altnet/BDE parties 'are financially intertwined such that one party's financial success is dependent upon the other'. They cited four features of the relationship:

(i) the agreement to share revenue (cl 5.1 of the joint venture agreement);

> (ii) documents filed by BDE with the SEC show that, in the 12 months to 31 December 2003, over 90% of BDE's revenue came from activities dependent upon the availability of KMD to users;
> (iii) On 23 June 2003, BDE granted Sharman a warrant, exercisable until 23 June 2008, to purchase shares in BDE, at a fixed price;
> (iv) Altnet and BDE are linked, through cross-holdings, with Joltid, the licensor to Sharman of the PeerEnabler technology and KazaaLib file software.
> (v) A document discovered by Sharman, headed 'Altnet and Sharman Networks', states:
> *'In the course of developing Kazaa Media Desktop, Sharman Networks' relationship with Brilliant Digital and the Altnet system are essential. The technologies are so intertwined that they cannot be decoupled except at the most barest of technical levels. As well, the company's marketing strategies similarly related, so much so that the future success of Sharman Networks and the Altnet systems depend on one another.*
>
> *When designing future features of KMD, project managers from Sharman Networks works directly with BDE officers to align our project goals. Our visions for the combined effort and single user experience allow our companies to share responsibilities and act as a single unit.'*

122 This document goes on to speak about 'developmental integration' and 'technical integration', both of these concepts being said to involve a series of co-operative steps between the two companies. The document envisaged that either company might draw up a specification for a future feature, or enhancement, of KMD, that this specification would be sent to the other company and a telephone meeting would then be

convened to discuss and progress the proposal.

123 The evidence does not identify the author of this document. However, having regard to its provenance, it is admissible as a business record: see *Evidence Act 1995* (Cth), s 69D. It provides evidence of the matters stated in the document. The weight to be given to the statements is a separate issue. However, having regard to the fact that the statements are not inconsistent with other evidence in the case, and have not been refuted by the respondents, it seems appropriate to proceed on the basis that they are correct.

124 In their Closing Submissions, counsel for the applicants cited numerous documents evidencing close co-operation, in practice, between Sharman and Altnet officers, including between Ms Hemming and Mr Bermeister.

125 Counsel also pointed out that cl 3.5 of the joint enterprise agreement required Sharman to ensure that Altnet's TopSearch function was installed simultaneously with the KMD technology and that KMD will cease to function if a user removes TopSearch. Counsel said:

> *'The technical integration of the TopSearch function into the KMD is so pervasive that users do not distinguish between KMD and Altnet. KMD is a single piece of software which is supplied. One can identify in a motor vehicle different features such as the engine or brake pads which, in a different form i.e. without the connecting bits, could be supplied separately, but in fact form part of a single package, namely the car. Similarly, one can trace the different capabilities of the Kazaa software to software applications which could, as a matter of theory, be supplied separately without the connecting bits, but which in fact are supplied as part of and embedded in a single piece of software.'* (Footnote omitted)

126 Counsel for the applicants pointed to evidence about personal relationships between Sharman and Altnet officers. Companies controlled by Mr Bermeister previously employed both Ms Hemming and Mr Morle.

127 I have already noted that, according to Ms Hemming's Answers to Interrogatories, Mr Bermeister was instrumental in her acquiring the Kazaa business. Her decision to make that acquisition presumably resulted in Sharman being formed. The evidence does not reveal whether Mr Bermeister was involved in that event.

128 Mr Morle worked for Brilliant Interactive Ideas, a subsidiary of BDE, from October 1999 until early 2001. From early 2001 until early 2002, he worked directly for BDE, being responsible for its web design work for third parties. In January 2002, Mr Morle left BDE to become LEF's Director of Technology. In evidence, Mr Morle recounted an interview he had with Ms Hemming, during which Ms Hemming telephoned Mr Bermeister to discuss Mr Morle's proposed move to Sharman. Mr Bermeister gave 'his blessing'.

(v) The technical experts' agreed propositions

129 Prior to commencement of the hearing, I requested that the technical experts who were to give evidence confer together and attempt to reach agreement, to the maximum possible extent, about the technical issues raised by their affidavits. A conference did take place, although not until well after the hearing had commenced. It resulted in agreement about some matters. The agreement was recorded in a document signed by the experts that was called 'Agreed Propositions by Technical Experts'. It became exhibit G. The agreed matters were:

'1. Any type of file may be placed in "My Shared Folder" and, in particular, any type of music file (including wma and mp3).

2. The sharing function of "My Shared Folder" can be disabled by the user.

3. If a gold file is subject to DRM, it will be necessary for the user to obtain a licence before the file can be played fully.

4. By default, blue files downloaded by a user are placed in the "My Shared Folder" and are available to other users.

5. KMD orders the results from two searches and determines the placement of blue files and gold files in search results presented to the user.

6. Whenever KMD connects to the Kazaa website, it is possible for the website to collect the IP address of the node running KMD, or if that node is behind a Network Address Translator, of the address presented by the Translator.

7. IP addresses are often dynamically assigned – they can change every time a user connects to the Internet. Many IP addresses are statically assigned. To link a user to an IP address at any given time, you would need information from the user's provider.

8. The Kazaa UI contains:

2. an optional keyword filter that allows a user to insert words of his or her choice;
3. an optional keyword filter for adult or offensive content.

9. Sharman from time to time has released new versions of KMD, which users may choose to install.

10. It would be possible to redesign the Kazaa UI so that:

> *(c) the keyword filters were non-optional;*
> *(d) the keyword filters included metadata such as names of artists and song titles;*
> *(e) the keyword filters included Boolean combinations of metadata;*
> *(f) files with .mp3 extensions were not displayed; however,*
> *(g) the introduction of such filters would not prevent the distribution of some unauthorized material (including music files) using KMD; and*
> *(h) the introduction of such filters would prevent the distribution of some authorized or public domain material (including mp3 files) using KMD.'*

(vi) The relationship between gold and blue files

130 In para 5 of exhibit G, the experts agreed that 'KMD orders the results from two searches and determines the placement of blue files and gold files in search results presented to the user'. Counsel for the

applicants argued the evidence justifies the conclusion that, although separate searches are made for gold files and blue files, there is a close connection between gold files and blue files, enabling the Altnet respondents (and therefore the Sharman respondents) closely to monitor users' blue file requests. In their Closing Submissions, they said:

> *'Attached to each Gold File is metadata which includes not only the usual information about the file such as file title and artist but also is a list of "keywords".*
>
> *Altnet prepares an index of all available Gold Files including their metadata which in turn includes their respective keywords. This index is the "TopSearch index". Altnet updates the index on a regular basis to coincide with changes in the list of available Gold Files and with changes in keyword matches for existing Gold Files.*
>
> *The Kazaa software is designed so that the updated TopSearch index is regularly pushed down from Altnet controlled computers to Kazaa user's computers. Such communications are possible because the Altnet computers are aware of the IP addresses of the Kazaa users' computers which are connected to the system at the time of those communications.*
>
> *The presentation of the Gold File results as part of the search results presented to a Kazaa user in response to his search request is achieved as follows. As well as being sent to its relevant supernode, a Kazaa user's search request is sent at the same time to the "TopSearch index" in the Kazaa user's computer.*
>
> *Because the search request is the same as that sent to the supernode, the logical conclusion is that it is the same encoded communication as that sent to the supernode. The fact that the TopSearch index can interpret that communication inevitably leads to the conclusion that Altnet has access to the source code relevant to the communication between the node and the supernode.'* (footnotes omitted)

Counsel suggested this source code is the source code attached to a document (exhibit H) called 'Kazaa Lib API programming' ('API').

131 Counsel submitted:

> *'At the supernode the search request is matched against the metadata including keywords related to Gold Files. If there is a match with any part of the metadata or any of the keywords associated with a Gold File, the relevant Gold Files are presented in the search results provided to the Kazaa user. ...*
>
> *The keywords attached to a Gold File which trigger a matching search result with a search request need not bear any relation to the content of the Gold File. For example, a commercial provider of Gold File content could have its Gold File associated with a keyword which consisted of common search requests by Kazaa users, for example the name of a very popular musical artist, although the Gold File content had nothing to do with the works of that artist. The benefit of using that keyword would be the regular notification by way of search results to Kazaa users of the availability of that Gold File.*
>
> *In its dealings with potential third party Gold File content providers, Altnet relies on its ability*

to link the words of popular search requests with Gold Files which it is trying to sell for its clients. Those popular search requests are for words related to the Applicants' popular sound recordings.

In filings with the Securities and Exchange Commission in the USA, BDE has stated that a significant feature of the Altnet network is its ability to communicate with Kazaa users on computers worldwide as a result of which the "tens of millions of search requests each day" made by Kazaa users "can be intercepted by Altnet" so that "secure content provided via Altnet can be made visible to Kazaa users". These assertions, made in circumstances where falsity exposes one to penalty, should be accepted as correct; and should prevail, where in conflict, with assertions by experts who only looked at the software from the outside.

In its marketing documents Altnet says that its system provides:

> *"The ability to listen to 120 million search requests per day on Kazaa and return secure keyword-indexed, DRM-protected results into the Kazaa desktop."'*
> (footnotes omitted)

132 Counsel submitted the 'better view of the evidence is that the TopSearch functionality within the Kazaa software **presently** enables the identification of the terms of every search request by a Kazaa user by reference to that user's unique inactive machine ID' (counsel's emphasis). They cited the following considerations:

(i) the conclusion is supported by BDE's statements to the SEC;
(ii) nobody from Altnet or BDE gave evidence contradicting that conclusion, despite the fact that the proposition was asserted by the applicants before trial and in opening submissions;
(iii) 'an ability to monitor search requests by Kazaa users is the natural conclusion to be drawn from Altnet's stated object of selling popular keywords to potential Gold File content providers';

(iv) Altnet's obligation, under cl 4.8 of its joint enterprise agreement with Sharman (see para 118 above);
(v) evidence given by Rodney McKemmish, a computer forensic expert called by the Altnet respondents; and
(vi) the lack of evidence establishing the content of the Kazaa source code and, therefore, that it would not enable reporting back of blue file searches.

133 The SEC submission included the following statement about Altnet's ability to intercept Kazaa search requests:

'A significant feature of the Altnet network is its ability to communicate with FastTrack technology already installed on desktops worldwide. Tens of millions of search requests each day are being made on the FastTrack Network via the KaZaA Graphical User Interface (GUI). These search requests can be intercepted by Altnet and returned to the FastTrack Network and displayed in the KaZaA GUI such that secure content provided via Altnet can be made visible to KaZaA users. Altnet has reached an agreement with Sharman Networks to allow Altnet search results to propagate in the KaZaA GUI and Sharman Networks has indicated its intent to work with Altnet and Altnet's customers to highlight secure search results so as to increase

the popularity of the underlying content.''

134 That statement is consistent with one made in an Altnet marketing document 'Altnet Value Proposition'. In summarising the advantages gained by an Altnet licensee (content owner), the document referred to:

'The ability to "listen" to 120 million search requests per day on Kazaa and return secure keyword indexed, DRM-protected results into the Kazaa desktop'

135 Mr McKemmish had studied, and claimed to understand, the TopSearch source code. He said it enables the Altnet server to identify the located file in respect of 1% of all successful gold file searches. Mr McKemmish was asked whether it would be possible 'to have a report back of what the user is looking for regardless of whether it is successful'. He replied 'it would need some changes to the current code to do that'. Mr McKemmish was then asked whether it would be possible to modify TopSearch so that it would report back to Altnet that somebody had searched for an artist or title that was not a gold file. He said this could be done.

IV MAJOR FACTUAL ISSUES IN THE CASE
(i) Knowledge and intention
(a) Documentary evidence

136 Counsel for the applicants tendered documentary material that, they said, demonstrated the respondents' knowledge that the Kazaa system was being used extensively for the purpose of transmitting copyright material. They also said the documents showed the respondents intended it should be so used; or, at least, that they had no wish to curtail that use.

137 By the end of the trial, there was no real dispute about knowledge. Nonetheless, it is necessary to note the nature of the material. The nature and extent of the respondents' knowledge is argued to support an inference about their intention. There is dispute about intention.

138 Some of the documents are undated; so those discussed below will not necessarily be in chronological order.

139 The first document to be mentioned is dated 18 January 2002, three days after the incorporation of Sharman and about the time that Ms Hemming and Mr Morle commenced to work for that company. It is an Altnet document entitled 'Altnet Presents Peercast'. The third page of the document reads:

'Our mission is to

***CREATE** a scalable framework onto which a broad range of P2P services can be built, both by ourselves and by partner companies.*

***BUILD** a robust set of P2P network interface components with a flexible API and powerful authentication, security & reporting, providing a framework on which a large range of current and future applications can be built.*

***TRANSFORM** the world's largest existing user base of users into users of the new P2P platform, converting them from people sharing music files into subscribers, members and*

beneficiaries of a broad range of services built on top of a unified P2P platform.

***MONETIZE** the existing P2P user base and our intellectual property investment via a range of selected P2P-based applications which have an immediate revenue potential.*

***PROVIDE** an online exchange in which we can match the requirements of partner companies (resource requesters) with the resources (CPU, bandwidth, storage and more) made available by the millions of users on the P2P network (resource providers).'*

Counsel for the applicants emphasised the third objective. That objective is similar to the purpose underlying the formation of Altnet notified to the SEC: see para 108 above.

140 Page 5 of this document contains this statement:

'As we build a new network with a new set of applications, an important design goal will be the migration of the existing user base to the new set of applications and services. The challenges comprise legal (the old network carries copyright-infringing material), technical (new applications need to be seamlessly provided to millions of users), architectural (the new network needs to provide a broad range of services) & backwards-compatibility (new services should ideally be able to take advantage of the existing Share Folders maintained by existing users).'

The next paragraph identifies the 'old network'. The paragraph says 'there is only one network, shared by both legacy (KaZaA Media Desktop) and new applications'.

141 Shortly after the date of this document, in early February 2002, Mr Rose worked with Priit Kasesula of Bluemoon in preparing a document called 'Proposal and Specification for TopSearch P2P Search Result Highlight System'. It seems the first draft of this document was prepared by Mr Rose. Mr Kasesula made some comments. Mr Rose responded. Finally, Mr Rose added a statistics reporting section.

142 In the body of the document, there was a section called 'KMD reporting'. Mr Rose's proposal was for a 'stats reporting module' for the KMD player that would record users' activity in relation to 'sponsored files' (presumably gold files). These statistics would be made available to some third parties, presumably sponsors and advertisers. Mr Kasesula commented:

'Posting stats to 3rd party servers will open up potential security issues like them collecting IP addresses of all the clients
Reporting will make KaZaA a 'spyware', as soon as it becomes evident that we record downloads and playbacks users will flee to competitive networks.
And 3rd issue is legal issue that stats might open up. One can argue that we have knowledge of copyrighted material being downloaded in our network and have to install filters.
Of course we won't know about downloads and playbacks of non signed content but it doesn't make [a] *difference because*

1. it is hard to communicate this to users and lawyers
2. if we are reporting signed files, then technically we could do same for any file
Anthony: See Reporting section below.'

143 The section on reporting statistics, later added by Mr Rose, includes the following:

> *'Having specified **what** stats are being reported, the question is **where** these stats should be reported to. The options include:*
>
> *1. Simply post each stat individually directly to a central stats server.*
>
> *2. Store all the user's stats locally on the user's machine, and then each time the user starts KMD (or at other periodic intervals) send the accumulated stats to a central stats server.*
> *3. Send each stat back to a supernode (or some subset of the available supernodes) – these supernodes then batch together the stats from hundreds or thousands of users and send them to a central stats server.*
>
> *One important issue that must be addressed is **privacy**. If you think of a highlighted search entry as being equivalent to a banner ad then in theory there shouldn't be any privacy issues – users are already aware that each time a banner ad appears (and again if they click on it) it sends a stat to DoubleClick's stats server, and if our stats are identical in the information that they report then there should be no issues, right? Unfortunately it won't be that easy, for these reasons amongst others:*
>
> *- When a stat is reported to a web server it necessarily includes the user's IP address. This is no different to the stats reported by banner ads, so that if a user was browsing a porn site then in theory DoubleClick could log that behaviour. However, in the P2P space that tracking has not previously existed, and perhaps users take advantage of the greater anonymity. Suddenly adding a mechanism that allows IP address to be logged when you search for a particular file (maybe even any copyright-infringing file) might be objectionable to users (although it should be pointed out that their IP address is publicly viewable if they then share that file out on their machine).*
> *- Unless we explain to users exactly what information is being reported, users might fear the worst and assume we're tracking all searches, not just highlighted searches, or that we're sending additional user information to a central server – this could cause a user backlash.*
> *- The system could be misused by, for instance, the RIAA running a highlight campaign which allows them to collect the IP address of everyone who has searched for or downloaded that file.*
>
> *These are complex issues requiring business vs. privacy vs. implementation time tradeoffs – we can discuss this by phone.'* (Original emphasis)

144 Counsel for the applicants argued these exchanges made several relevant points:

(i) the display of a 'banner ad' on a user's computer generates 'a stat' identifying the user's IP address, which is recorded. The evidence shows that banner ads are continuously displayed on KMD users' computers;
(ii) it is possible to capture and record the IP address of a user who receives a search result, not only of a gold file but also a blue file, and to record whether that user downloads the file;
(iii) establishing such a system would be unpopular with users;
(iv) such a system 'could be misused' by the record industry to identify the IP addresses of

copyright infringers;
(v) under such a system, a user's action in sharing a file would result in the sharer's IP address becoming publicly available; and
(vi) logging an IP address will identify a Kazaa user.

145 It is not clear how Mr Rose and Mr Kasesula resolved the problem they discussed. But it is interesting to note an email of 26 June 2003 from Mr Rose to Tommaso del Re of Sharman regarding 'Streamwares performance metrics'. The email reads: 'For various legal reasons it's better that you don't email me asking for stats on audio files'. As neither Mr Rose nor Mr Re was called, there was no opportunity for counsel to obtain an explanation of this email.

146 Another Altnet document (undated) is a presentation to Interscope, a subsidiary of Universal Music which holds copyright in Eminem sound recordings. The title sheet on the presentation document read:

'ALTNET
In the time it takes to make this presentation, 365,000 Interscope tracks will be downloaded without paying you one cent.
ALTNET can change that'

The final page of the presentation included the statement:

'With ALTNET, record labels can reach over 100 million music fans presently downloading 3 billion files per month.'

147 A further undated Altnet document is headed 'Altnet Digital Marketing Proposal'. Page 2 contains this material:

'What is ALTNET?
Altnet leverages KaZaA, the largest content audience on the Internet
☐*Over 60 million users (Larger than AOL!)*
☐*120 million content-specific search requests per day*
☐*2+ million users online at any given moment*
☐*Growing by 2.5 million new users every week*
☐*Over 3 billion files downloaded each month'*

148 On 16 April 2003, Mr Morle sent an email to two other Sharman employees detailing the growth in file sharing. His statistics included the following information:

(i) 25 August 2002 at 6pm
1.8 million users online
316 million files being shared (175 per user)

(ii) 7 January 2003 at 11.30am
3.6 million users online
702 million files being shared (195 per user)

(iii) 10 April 2003 at 2.31am
3.7 million users online

828 million files being shared (223 per user)

149 On 24 April 2003, Altnet proposed the conduct of some focus groups by Syzygy Branding ('Syzygy'), a market research company. On 23 May 2003, Syzygy reported the outcome of the focus group meetings. Its report noted that 'Kazaa' (presumably Sharman) was 'preparing to launch a new version of its application featuring several new design elements and features'. The document reported that four focus groups of Kazaa users had each met for one hour. All four groups comprised young people (up to 25 years of age).

150 The methodology section of the report stated:

> *'An initial discussion was conducted as to perceptions of music downloading attitudes and behaviours, etc. prior to exposing respondents to the new application.'*

151 The report's summary of conclusions included the following:

> ***'Perceptions/Use of Kazaa**:*
>
> *- Kazaa is currently thought of as a free music downloading search engine*
> *- Though consumers use it on a consistent, high frequency basis, the relationship is currently limited to a narrow process:*
>
> *- I know the song I want*
> *- I go to Kazaa to download it for free, with no hassles, at no cost*
> *- I burn it on to CD to play in my car, etc.*
>
> *- Kazaa offerings that go beyond music, seem complex, require payment, or position the site as a place to linger will likely encounter initial acceptance hurdles and require significant effort in repositioning, consumer awareness and education'*

152 The report included a section headed 'Blue and Gold Icons'. That section included the statement:

> *'Substantial hurdles exist to paid-for content, respondents seemed likely to search for blue version of the same song to avoid payment despite quality/virus issues, etc.'*

153 The recommendations section of the report included the following statement:

> *'Music is at the heart of Kazaa's identity, and straying from this content area threatens to confuse and alienate users unless the groundwork has been laid to do so.'*

154 In a findings section, the report stated:

> *'Typical behaviour is to:*
>
> *- Hear a song (radio, friend, etc.)*
> *- decide they want it*
> *- go to Kazaa specifically to get that song*

Many respondents stated that they use free downloading as a precursor to purchasing a CD, preferring to know what they are buying by sampling the full complement of a CD's songs on-line first. Respondents complained of buying CD's and finding they only had one good track.

Though some respondents did use music downloads and streaming to soundtrack their computer experience, the overwhelming behaviour was to download, burn CD's and use the music in other players, (particularly cars) for those old enough to drive.

Frequency of music downloading behaviour was high. The majority of respondents indicated daily use.'

155 The Sharman respondents produced a copy of Syzygy's report, during the discovery phase of this proceeding. Copies of the report had apparently been provided to all the present respondents. Certainly, they were all told about the focus groups. On 18 May 2003, Mr Bermeister sent an email to Ms Hemming, Mr Morle and others, with copies to Mr Rose and two other people, reporting what he had learned by attending the four focus sessions held that day. The email referred to the Peer Points system, rewarding users for file sharing. Mr Bermeister said:

'*The outcome of the groups for me (for Peer Points) is to shift our messaging away from a mainstream message to an even more focused message directed to the "geek" group that is likely to get into the game of files sharing first. I see our current messaging as "sharing files on Kazaa ... now get paid to do it" shifting to something like "become the biggest file sharer in the world and win $1m". It is more likely that the "geek" group will pick up on the relevance of this faster and if the messaging is more oriented toward this smaller group I get the feeling that the "I can't win" notion will be watered down.*

We will send a video of the session to you on Monday. A comprehensive analysis of the sessions to follow. Your sessions will be able to cover any of the issues we missed over here.'

156 Shortly after this research project, Sharman received a 'Creative Strategy Brief' from an organisation called 'Magnet', apparently a marketing consultant. The document referred to a 'Consumer Education' campaign. It included the following background statements:

'☐ ***Kazaa*** *is the brand name of the leading "peer-to-peer" (P2P) file sharing software in the world. Kazaa is owned by* ***Sharman Networks, Limited (SNL)****, an Australian technology company.*

• Through Kazaa, users go online and exchange digital files (e.g. music, games, software) through a "network" that allows users to "share" files over the internet by accessing a "file folder" that exists on the hard drives of other user's computers. There is no central server – all files are exchanged between individual user's computers, which is called peer-to-peer.

• ***Kazaa Media Desktop (KMD)*** *is the application that users download to their computer to enable file sharing. Through KMD, users can use a keyword search to locate desired files on another computer, and then download those files to their computer. Also, through their own "shared folder" KMD users provide other users access to the files they have downloaded and kept.*

• KMD is a state-of-the-art technology affording users maximum anti-viral protections and privacy safeguards. Kazaa is committed to protecting user privacy and providing a secure and safe platform.

• SNL's revenue is derived from online advertising on the Kazaa Media Desktop and through "channels" that allow creators to package their work for distribution through KMD. There are currently more than 100 million users of Kazaa Media Desktop worldwide who are engaged in file sharing on the Internet.

*• Through a partner, Altnet, Kazaa offers users the opportunity to pay a "digital rights fee" to download copyrighted materials for their own personal use. These files are identified on Kazaa with "**Gold Icons**" and users can purchase rights to download these files from Altnet with a credit card.*

• The goal of SNL is to evolve Kazaa into a file sharing platform where users can both purchase *copyrighted material and* share *non-copyrighted material through the P2P network.'*

157 The first item discussed under the heading 'current issues' was copyright infringement. The discussion commenced:

'• Because Kazaa allows open sharing of files between users, the P2P network enables users to exchange copyrighted materials (e.g. music and video files, published documents, games and software) without paying the owner of the protected content, which is illegal copyright infringement.

• Kazaa has come under attack from the music industry (Recording Industry Association of America – RIAA) and the movie industry (Motion Picture Association of America – MPAA)

• The music industry (in particular) claims that illegal file sharing of downloaded copyrighted material has caused great economic harm to the industry, and to the artists who own the rights. Over the past 2-3 years there has been a 20% decline in the sale of CDs, which the RIAA attributes to file sharing (without evidence to prove file sharing is the cause).

• However, the music industry has refused to view P2P file sharing as a legitimate platform to distribute music files for commercial sale, which has resulted in limited content available for sale through Kazaa/Altnet.

158 Reference was then made to the Grokster litigation in the United States. The document included a proposal for an advertising campaign that included this objective:

*'To **migrate** users of KMD (present and prospective) to consider trial of Kazaa as a platform for purchasing quality (music, games, software) files legally, while continuing to share unprotected content for free.'*

159 The documents tendered in evidence include an email dated 4 October 2003 from Damien Petty, apparently a consultant, to Mr Bermeister, with copies to Derek Broes, apparently of Sharman, and Ms Hemming. Mr Petty attached 'a version without logos', with Altnet's name removed from the text. Although I cannot be certain of this, it appears the attachment was a document (also in evidence) that was intended to be presented at a conference being held at that time. The document was entitled 'Saving the Music Industry – Proposed Business Model for Digital Music Distribution'. It was designed to persuade participants in the music industry that they should come to an agreement with Internet file-sharing companies for licensing their copyright works. The first sheet of the document referred to the recent decline in United States retail music sales. It included a quotation from Mitch Bainwal, who was identified as 'CEO of RIAA' (the United States Record Industry Association):

> *'the root cause for this drastic decline in record sales is the astronomical rate of music piracy on the Internet ... Computer users illegally download more than 2.6 billion copyrighted files (mostly recordings) every month. At any given moment, well over five million users are online offering well over 1 billion files for copying through various peer-to-peer networks.'*

160 Material prepared for a presentation by Ms Hemming at the same conference included a graph showing that, in the week ended 16 February 2003, KMD accounted for 79% of weekly downloads, as against only 21% for all other Internet file-sharing companies combined.

161 Other interesting documents include an exchange of emails on 19 November 2003 concerning a request for information by six United States senators. The questions were:

> *'1) Will your company take responsibility for educating consumers by immediately beginning to provide a clear, conspicuous, and meaningful warning to users, before they download your software, that using the software to "share" copyrighted music is clearly illegal under existing law, and doing so may subject them to lawsuits like the ones recently filed by the RIAA?*
>
> *2) Will your company incorporate effective copyright and pornography filters into your software in an effort to reduce or prevent copyright infringement and illegal access to pornography?*
>
> *3) Will your company help users avoid copyright liability by changing the automatic "sharing setting" in their P2P software [so] that users are required affirmatively to choose to share files instead of being required to as a default?*

162 Ms Hemming apparently passed on the questions to Mr Bermeister. On the same day, he emailed to express 'my views':

> *'1. yes – subject to laws of each country*
>
> *2. yes – subject to there being little or no impact to user experience and provided you recognize the existing adult "filter" which the questions fails to recognize*
>
> *3. no – p2p exists by virtue of this feature being turned on*
>
> *my expectations*

1. this will gave [sic] little or no impact on users

2. this will never come together provided the obligation is on them to provide a filtering system

3. they won't come back on this because on the public record it seems like an unreasonable request.'

(b) Mr Morle's evidence

163 Mr Morle made an affidavit dated 24 November 2004 which commenced with a brief history of his career. Mr Morle was born in England where he developed an interest in the performing arts. After he left university in 1989, he became Artistic Director of a London theatre company called KAOS Theatre. In 1994, KAOS Theatre established a second company in Western Australia and Mr Morle moved to Perth to manage its activities. While living in Perth, Mr Morle subsidised his income by designing and building websites. He already had some familiarity with computers; his father and brother were both employed in the computer industry. In 1999, Mr Morle decided to make web development his career. He obtained a position with Access Systems in Sydney.

164 After about six months, Mr Morle moved to Brilliant Interactive Ideas ('BII'), a subsidiary of BDE. In that capacity, he was instructed, in about September 2001, to work on a new website for Kazaa BV. Mr Morle understood Kazaa BV to be a new client of BDE.

165 Over the period from September 2001 to January 2002, Mr Morle worked on a redesign of the Kazaa BV website, the focus being on 'the look and feel', rather than the content, of the site.

166 BII went into administration at the end of 2001. By that time, Mr Morle had met Ms Hemming, who worked in a nearby office at Darling Harbour, Sydney. On about 21 January 2002, Mr Morle said, Ms Hemming called him into her office. She told him she was starting a new company, called LEF Interactive. It would be a technology services company and a large client would be Sharman, a company that had recently purchased the Kazaa application and website domain. Ms Hemming offered Mr Morle a position as Director of Technology with LEF. She told him his services would be sub-contracted to Sharman. Mr Morle said:

'I was told that ... the mission of Sharman was to commercialise peer-to-peer ("p2p") software. The approach, I was told, was to provide high quality, paid, DRM ("Digitally Rights Managed") protected files in search results that users would prefer over files that other users may choose to share. I was also told that a BDE subsidiary called Altnet would provide the DRM protected search results. I was already aware of Altnet as a consequence of my employment at BII.'

167 Mr Morle accepted Ms Hemming's offer. As BII was then in administration, Mr Morle was available to start immediately. Ms Hemming telephoned Mr Bermeister. He agreed to Mr Morle doing that. Apparently, Mr Morle commenced with LEF about the end of January 2002.

168 Mr Morle said he has never signed a formal employment agreement with LEF. He claimed to have no financial interest in any of the Sharman companies. He said he received only normal employee entitlements such as salary and superannuation.

169 Mr Morle said that, when he commenced with LEF, the only other people working for Sharman were Ms Hemming, who 'as CEO is at the top', and Mr Morris, who was then located in London. Mr Morle said Mr Morris was Executive Vice President and second in charge. However, shortly after Mr Morle commenced with LEF, two programmers were employed, and then Michael Liubinskas, as head of marketing. By the end of 2002, there were about 12 employees. The number has since increased.

170 Mr Morle described the structure of the 'Technology team', which he leads. He said he has no budget. He makes decisions involving spending up to about $3000. He refers to Ms Hemming in relation to larger amounts. Mr Morle claimed never to have seen revenue statements and to have no idea 'how much money Sharman brings in either globally or from any particular source'. Mr Morle claimed to have had no involvement in commercial negotiations; he said he only became involved if a technical issue arose.

171 Mr Morle dealt in his affidavit with copyright infringement. He said:

> *'On my first day working for LEF Nikki explained to me that various changes were to be made immediately to the website at www.kazaa.com and the web pages accessed from the KMD to remove elements of the site that might potentially encourage copyright infringement. I was given specific tasks to do to achieve that end including the following:*
>
> > *(a) powering down the Kazaa servers so that the website went off-line;*
> >
> > *(b) removing the discussion forum to prevent users encouraging each other to engage in copyright infringing activity;*
> >
> > *(c) adding copyright infringement warnings to the website – I was provided with a specific wording to use which, as far as I recall, is the same or similar to the current warning that exists at the bottom of the Kazaa.com homepage;*
> >
> > *(d) updating the End User Licence Agreement – I do not recall precisely what the content of the Agreement was but as far as I recall it included conditions of use to the effect that users were not to infringe copyright;*
>
> *I did all of those things as instructed. Additionally although my recollection is not firm it is that I also removed the help pages and the links to those pages, in case they provided any instructions which might encourage copyright infringement.*
>
> *At the end of this exercise all that was really left of the Kazaa.com website was 1 page with a link to the End User Licence Agreement. Once it was reduced to this bare minimum we re-developed the site over the coming months.'*

172 Mr Morle said he added Altnet's TopSearch to KMD 'within a couple of months'. He claimed that, since commencing with LEF, he had made inquiries of various people and conducted research about 'copyright filtering'. He explained this term as meaning 'technological measures or enhancements which could be introduced so as to prevent the use of Kazaa to participate in a system of copyright files which were not authorised for copying'. Mr Morle said he has 'yet to find a feasible solution'.

173 When Mr Morle was called for cross-examination, Mr A J Meagher SC, senior counsel for the Sharman respondents, tendered portion of an affidavit Mr Morle had made on 16 February 2004 ('Mr Morle's first

affidavit'). This affidavit contained a description of the Kazaa technology. It made claims that none of the respondents:

> (i) 'have any input or control over the searches that users of the KMD application perform with KMD software, nor over the files that users download with the software'; or
>
> (ii) 'make any copyrighted content available on-line to be searched and downloaded with the KMD application'.

174 Mr Morle described Altnet as 'third party software that delivers secure rights managed files by way of preferential search results in response to a user's request'. Paragraph 18 of Mr Morle's first affidavit described how this occurred:

> *'KMD contains Altnet's TopSearch and Peer Enabler technology. I am aware that Altnet's TopSearch application is also operating together with the Grokster peer to peer application. In general these components work as follows:*
>
> > *18.1 When a KMD user performs a search with the KMD application, the query is sent to the FastTrack software and the Altnet TopSearch software independently.*
> >
> > *18.2 If the request for a file by the user is one of the works licensed through Altnet, the Altnet file will be displayed on the KMD GUI with a "gold icon". This signifies to users that it is a licensed title.*
> >
> > *18.3 Gold icon files are displayed at the top of the search results ahead of all other search results (ie. the results from peer's computers) and may also be interspersed among other search results. This is like sponsored listings in Google searches.*
> >
> > *18.4 If there are a number of search results, it is up to the user as to which search result they select.*
> >
> > *18.5 If the user decides to download the gold icon file, he or she follows the normal download procedure. If no other Altnet user has the file, it will come directly from the Altnet server. If a KMD user decides to obtain a file from another peer, they will download the file from other user's computers, peer-to-peer.*
> >
> > *18.6 Once the file is downloaded and the KMD user tries to open the file, the terms and conditions for opening will be displayed. For example, the user might be required to make a payment before opening. Also, the user might be limited in whether the file can be copied to another device (e.g. a CD burner) or opened for play more than once or beyond a certain period of time. I am aware that the Altnet software within the KMD application contains procedures for facilitating payment.*
> >
> > *18.7 After downloading, the gold icon file remains in the user's shared folder so it can be found by other Altnet users. The Altnet software keeps track of when a gold icon file is downloaded from a user's computer, and Altnet provides "points" – redeemable for awards – to users that supply gold icon files to other peers from their computers to encourage the exchange of rights managed files.'*

175 During cross-examination of Mr Morle, Mr A J L Bannon SC, senior counsel for the applicants, asked about a proposal of a Sharman programmer, Rob Sanders, to collect information about the number of Kazaa users. Mr Morle agreed this information was collected, although he said the count was taken from FastTrack; not all the counted people were Kazaa users. Some of Kazaa's competitors also use FastTrack. Mr Morle did not agree the count was made by a software system that was separate from the Kazaa system. However, he did agree that Sharman had installed a special command, in the software used in its own computers, that screened out advertisements and provided the user number information.

176 Mr Morle was asked about a 'bank of computers' that was said to be in Denmark and that recorded user patterns. He said there had been a Kazaa web server in Denmark, supporting the Kazaa website system, but he claimed this had been shut down. In court, at Mr Bannon's request, Mr Morle connected to a particular website address which, Mr Morle acknowledged, was located in Denmark. It was not evident, from the demonstration, that the webserver was performing any useful function. Mr Morle explained later it was a remnant server which continued to receive data as to the number of users accessing Kazaa at any particular time.

177 Mr Morle agreed he was a member of the Sharman executive team. He knew about the focus groups conducted by Syzygy in May 2003. Mr Morle agreed the participants in the focus groups had openly stated they were using Kazaa to download copyright music and this conduct breached the terms of the users' licence agreement. Mr Morle was referred to a statement in the focus group summary: 'Kazaa is currently thought of as a free music downloading search engine'. He said he could not recall this in the document but he agreed this expressed his understanding of users' perceptions.

178 Mr Morle knew about a 'Join the Revolution' campaign launched by Sharman in September 2003. He agreed the campaign included distribution of photographs of a person wearing a T-shirt that bore the following words:

'THE
KAZAA
REVOLUTION

30 years of buying the music of [sic] *they think you should listen to.*
30 years of watching the movies they want you to see
30 years of paying the prices they demand.
30 years of swallowing what they're shoveling.
30 years of buying crap you don't want.
30 years of being sheep.

Over. With one single click.

Peer 2 peer, we're sharing files.
1 by 1, we're changing the world.

Kazaa is the technology.
You are the warrior.
60 million strong. And rising.
Join the revolution

KAZAA
Share the revolution'

179 At the conclusion of his cross-examination, I asked Mr Morle what was the source of the constantly changing numbers of online users shown on the Kazaa website. Mr Morle said: 'As I understand it, the numbers are passed around by the supernodes, they are not collected in one place'. My exchange with him went on:

> *'I can understand each supernode [might] report a statistic or series of statistics relating to the transactions that that supernode is involved with at that particular moment but somebody has to add up the numbers from each of the supernodes and put them in the right categories and I don't understand how the process is done? --- I don't think it needs a person.*
>
> *I mean a computer. I am sure no live human being adds the numbers up but there must be some mechanism for extracting the data on a moment by moment basis no doubt from supernodes and putting the numbers together to put on the screen? --- As I understand, it as I testified today, the supernodes effectively tell each other how many files each other are sharing and together - I am not sure how - it's added up but it does all happen on the supernode level and that's the reason I have been given as to why the number isn't 100 percent accurate. It's an important point.*
>
> *...*
>
> *Well, I still don't have any idea who collects the numbers from the supernodes. I've done no better than Mr Bannon in trying to get an explanation? --- Well, there is no central source and you probably will struggle to understand it. It's very, very complicated and I don't understand it, but that's how it works and, you know, it's inside another company's software.'*

180 In re-examination, Mr Morle gave this evidence:

> *'Do you have any understanding of how the supernodes talk to each other in the network? --- No.*
>
> *Do you have any understanding of what information passes between the various supernodes on the network to yield the numbers on the screen that any* [Kazaa user] *sees when he or she has the GUI open? --- I don't know.'*

(c) Conclusions about knowledge and intention

181 I have no doubt that, at all material times, each of the respondents was aware that a major use of the Kazaa system was the transmission of copyright material.

182 The evidence does not establish the number of people who use the Kazaa system at any particular time. In recent years, that number has apparently always been high. 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.

183 From time to time during the hearing of this case, counsel or a witness commented that Kazaa could be used in a non-infringing way. It was said that people might wish to share with others their own original literary or musical works, or they might desire to provide easy access to non-copyright works such as the plays of Shakespeare or poetry of Milton. In their Closing Submissions, counsel for the Sharman respondents referred to Project Gutenberg which, they said, 'contains 42,000 free public domain or licensed content files, including ebooks'. They said the ebooks include classic works such as *Don Quixote* and *Romeo and Juliet*, which may be shared using KMD. Counsel also mentioned Creative Commons, 'a method of licensing that allows users to distribute their own non-infringing material via the KMD, while still potentially maintaining some form of copyright protection'. There was no evidence how this is achieved but one witness, Phillip Cambouris, spoke of finding links from the Kazaa website to the Creative Commons website. Mr Cambouris also downloaded some MP3 music files made freely available by their copyright owners.

184 I do not doubt that some people use Kazaa only in a non-infringing way. However, it seems unlikely that non-infringing uses would sustain the enormous Kazaa traffic claimed by the respondents. The explanation of that volume of traffic must be a more populist use.

185 The evidence indicates that use is popular music. The focus group reports are revealing. Syzygy's summary of perceptions and use noted that 'Kazaa is currently thought of as a free music downloading search engine'. Consumers' relationship with Kazaa was said to be 'currently limited to a narrow process:

- I know the song I want.
- I go to Kazaa to download it for free, with no hassles, at no cost.
- I burn it on to CD to play in my car, etc'.

Syzygy noted likely resistance to 'Kazaa offerings that go beyond music, seem complex, require payment, or position the site as a place to linger'.

186 Nobody could read the Syzygy report without realising that, 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.

187 Copies of the focus group report went to Ms Hemming, Mr Morle, Mr Bermeister (who actually attended the focus group meetings) and Mr Rose. Mr Morle admitted reading the report. It may be inferred, the more readily because of their failure to give evidence to the contrary, that Ms Hemming, Mr Bermeister and Mr Rose also read the report.

188 There is other evidence as well. Mr Rose's email exchanges with Mr Kasesula proceeded on a common understanding that copyright-infringement was pervasive. Mr Bermeister's email of 18 May 2003 to Ms Hemming, Mr Morle and Mr Rose (amongst others) discussed ways of getting 'an even more focussed message' to the 'geek' group that they should increase file-sharing. I doubt that any recipient would have thought Mr Bermeister was referring to Shakespeare or *Don Quixote*.

189 Mr Morle, the only respondent who gave evidence, readily admitted he knew copyright infringement was rife. That is why, he said, he had 'spent a lot of time thinking about filtering and considering how that would be done'. That is also why, he said, he had discussed filtering with Ms Hemming. I do not accept he did either of these things. However, that he thought it necessary to make the claim is revealing.

190 At paras 78 and 86, I noted Kazaa website exhortations to users to increase their file-sharing. Increase in sharing was a fundamental theme of Kazaa's 'Join the Revolution' campaign (paras 81-84). It was also a major theme of Mr Bermeister's email comments on the focus group sessions (para 155 above).

191 It is understandable that the respondents would wish to increase file-sharing. Kazaa is apparently sustained by advertising revenue. It is a fundamental of advertising marketing that price is sensitive to the exposure likely to be achieved by the advertisement. The more shared files available through Kazaa, the greater the attraction of the Kazaa website. The more visitors to the Kazaa website, the greater its advertising value and the higher the advertising rate able to be demanded by Sharman. And what is more likely to attract large numbers of visitors to the website than music, especially currently popular 'hits'?

192 Theoretically, it would have been possible for Altnet to establish a paid access system that operated independently of unpaid access; gold files without blue files. However, the focus group discussions indicated such a system would have little appeal to Kazaa users. The benefit to Altnet of association with Sharman was twofold. First, Altnet was able to 'feed off' users' searches for blue files. If a user entered the name of a musical item or performer, seeking to obtain free access, he or she could be offered a selection of gold files that might be of interest to the user, having regard to the nature of the search. Any increase in the volume of blue file searches would be likely to increase the number of people who ultimately elected to take, and pay for, a gold file. Secondly, Altnet shared the advertising revenue received by Kazaa, the value of which must have been influenced by the volume of blue file sharing.

193 There is no evidence that any of the individual respondents, Ms Hemming, Mr Morle, Mr Bermeister or Mr Rose, benefited personally from any increase in Kazaa's or Altnet's prosperity. Some may have done so; according to him, not Mr Morle. However, it was presumably in the interests of all these respondents that their employer should remain active and prosperous; certainly, they had no contrary interest.

194 In short, I find that all the respondents knew the predominant use of Kazaa was for the sharing of copyright-infringing material. None of them had an interest to prevent or curtail that predominant use; if anything, the contrary. Each of the respondents was at least acquiescent in the use of Kazaa for copyright-infringing activities.

(ii) Technological controls
(a) Direct control through a central server

195 Sharman's ability to control – or, at least, to influence - the conduct of Kazaa users is the most contentious factual issue in this case. A major element in that issue was whether there is a Kazaa 'central server'.

196 It is desirable to state what the witnesses meant by the term 'central server'. It was common ground that a new user obtains the Kazaa software by logging on to the Kazaa website and pressing various icons. The software is then provided through a server controlled by Sharman. In one sense, that is a 'Kazaa central server'. It is a server maintained on behalf of Sharman and has direct access to the new user's computer. However, that is not what the witnesses meant by 'central server'. They meant a computer software system that enabled the respondents, or one of them, to control the user's subsequent use of the downloaded Kazaa software, especially the user's file-sharing activities. The respondents' technical witnesses, including Mr Morle, asserted that the Kazaa system does not include such an element in relation to blue files. Counsel for the applicants contested this assertion. Although unable to adduce direct evidence of the existence of a central server, they argued there were a number of circumstances pointing to that conclusion. The contest

about this matter is what the parties called 'the central server issue'.

197 In support of their position, counsel for the applicants noted the terms of the API document (exhibit H). This document was produced on discovery by the Sharman respondents. It seems to have been designed as an instruction manual. It purports to describe the Kazaa system. It contains, as an annexure, what purports to be the Kazaa programming source code, called 'KazaaLib'. However, no witness gave evidence that this is, indeed, the source code that operates the Kazaa system.

198 On page 6 of the API, a statement is made that usernames are registered within a specific realm. The document goes on:

> *'There are multiple realms, each running their own central Kazaaserver along with their own user database. Realms do not have separate networks – they all share a single network; realms exist just for user registration and identity purposes. Your KazaaLib will connect to one of the realms; the realm choice is hardwired into compiled code of KazaaLib. In most KazaaLib API data structures, user realm appears as a suffix of the username.'*

199 On page 7 of the API, reference is made to the 'arguments' required for connection of a new user, namely an email address and an election by the user as to receipt of a newsletter. The document states:

> *'Both are passed to Kazaaserver for inclusion into the user database. They are not directly used by KazaaLib, and their validity is not checked.'*

200 On page 8 of the API, reference is made to the situation where authorisation cannot be verified because the 'Kazaaserver could not be contacted'.

201 These statements were considered by one of the applicants' expert witnesses, Leon Samuel Sterling. Professor Sterling is Professor and Adacel Chair of Software Innovation and Engineering in the Department of Computer Science and Software Engineering at the University of Melbourne. Since receiving a Doctor of Philosophy degree from Australian National University in 1981, he has been involved in testing and research at many institutions, both in Australia and the United States, and has published widely in the field, amongst others, of software engineering. I thought him to be a fair and careful witness.

202 In a document (exhibit L) containing propositions that were advanced by the applicants' technical experts, including Professor Sterling, but not accepted by the respondents' experts, a reference was made to the existence of Kazaaserver. During the course of cross-examination, Mr M Leeming, junior counsel for the Altnet respondents, asked Professor Sterling about this. Professor Sterling said the sole evidence for Kazaaserver's existence was the API document. The cross-examination went on:

> *'So is this the chain of reasoning? You say by reference to functionality that you can see in the API document that whoever wrote that certainly thought there was such a thing as [a] Kazaa server? --- I think it's the other way round. I think the system was designed, and again my attempt in design level, so the overall system was designed with the belief that a Kazaa server would be present. The API document was constructed to allow people to refer to a Kazaa server and I don't know what in fact is happening but it was designed in an attempt for there to be a Kazaa server.*
>
> ...

What I want to put to you is that you know that although the document says that there's a central Kazaa server you know that that hasn't been implemented in any of the versions of the source code that you've seen. That's where I'm heading. Do you understand the proposition I'm going to debate with you? I'm not asking for a response but that's where we're going? --- This is a very complicated system because there's a division of other sets of software. I don't know if the Kazaa server isn't sitting inside the FastTrack network. I don't know a range of things because I haven't been able to look at that and so again I don't know very much about it. I saw evidence referring to a Kazaa server which led me to believe that it was designed with that in mind and I don't know one way or the other how it's actually working and I don't have the resources to be able to - I didn't have the time nor was [I] presented with a document to be able to satisfy myself.

So the first thing is you couldn't be definitive in expressing a view about the existence of [a] Kazaa server? --- No.

Because of the reasons you've just enunciated? --- Yes.'

203 Mr Leeming had Professor Sterling agree that, when he logged into Kazaa, he was not asked for a password or an email address. He was asked for a username, but there was no authentication process.

204 Mr Morle said in evidence that, to his knowledge, there was nothing that 'answers the description of a Kazaa server'; the first time he heard this expression was during this proceeding.

205 In Mr Morle's first affidavit, he stated that none of the (then) respondents 'provides any form of customer support for the KMD software'. He said the respondents (that is, the Sharman parties) provide to users only a fixed user guide and 'a set of Frequently Asked Questions, with responses on the Kazaa Website'. Mr Morle conceded, under cross-examination by Mr Bannon, that his affidavit made no reference to assisting users to deal with bugs. However, he maintained the affidavit was essentially correct; although users could send in bug reports they were referred to a website for assistance in solving their problems. As I understood him, Mr Morle was insistent that Sharman itself had no ability to rectify the bug by manipulating the user's software.

206 Mr Morle acknowledged that, at one time, Sharman collected users' email addresses. When asked how the addresses were collected, he said:

'There was formatted to the Kazaa user interface which asks the user if they would like to sign up for a newsletter and asks them for their email address as they did and that was displayed to the user when they first ran Kazaa. If the user did add an e-mail address to that form, that e-mail address was sent to a web server.'

207 Counsel for the applicants contended there was 'no satisfactory explanation ... as to why the computers collecting the email addresses did not constitute the Kazaa server'. They added that, if the Danish computers have been decommissioned, 'there is no evidence that they have not been replaced by computers elsewhere'. In any event, counsel said, there are 'Altnet servers which, on any view, are in direct communication with all Kazaa users'.

208 Counsel for the applicants submitted:

> *'The appropriate conclusion as to the appearance on a Kazaa user's screen of statistics as to the number of users online and the number of files being shared is that there is a central body receiving the individual statistics from individual computers and adding them together. Explanations which do not accept this are unpersuasive.'* (footnote omitted)

209 I agree with counsel's observation about the lack of a persuasive explanation as to the collection of statistics. During the course of the trial, several of the respondents' witnesses were asked to explain how it was possible for the Kazaa website to run a dynamic report of the number of persons currently online, if there was no central server counting those people. Mr Morle said the figure was actually of people using FastTrack, not all of whom would be using Kazaa. To the extent that is true, the website statement is false and misleading. However, Mr Morle's response does not solve the mystery; the respondents claim the FastTrack system also does not contain a central server.

210 Perhaps the most plausible suggestion offered by any witness was that the statistics are collected by communication between supernodes. An analogy was postulated of a group of fathers who formed a circle in a park. The first father told the second father he had two children; the second father added his three children and gave the figure 'five' to the third father etc. Once the counting had gone full circle, the last person could announce the total figure to the assembled fathers. However, if the analogy has any bearing on this problem, the result would also have to be communicated by one of the supernodes to Sharman. How?

211 More significantly, the envisaged group of fathers was relatively small and able to be formed into a static circle. That envisaged situation stands in marked contrast to the present question. There is an enormous number of supernodes in the Kazaa system and they are anything but static. Supernodes are constantly being opened up and closed down. No witness was able to explain, and I cannot imagine, how a progressive count between supernodes could be organised. If the claimed online figure has any validity, the most natural explanation seems to be that all the nodes (or at least all the supernodes) are constantly conveying use data to a central server.

212 In their Closing Submissions, counsel for the applicants referred to an email from Mr Rose to Mr Morle dated 4 April 2003. This email responded to a request from Mr Morle to Mr Bermeister to explain the rationale of having Altnet files download to a separate Altnet folder. Mr Rose gave reasons for this decision and explained:

> *'Based on the above, I engineered a system that met our business decision to keep two separate folders, but allows me to switch to using the Kazaa folder at any time, even post release, in case consumer feedback indicates users are having problems finding their Altnet files.*

213 Counsel said this passage shows Mr Rose was able, post-release, to control what occurred on a user's computer. They added:

> *'Rose's failure to give evidence as to the remote alteration capacity of the Altnet technology (or, indeed, at all) supports the inference in favour of the availability of forced updates.'*

214 In this context, by the term 'forced updates', counsel meant updates directly imposed upon users from outside, whether the users liked this or not; as distinct from updates that the users themselves accepted, even if only as a result of pressure. Counsel's point, as I understand it, is that a true forced update is possible only if there is a central server giving Sharman the ability to manipulate the user's computer software.

215 Counsel for the applicants also referred to a passage in the 'Altnet Presents Peercast' document referred to at paras 139-140 above. The passage was as follows:

> *'Most P2P applications consist of an EXE file architecture that requires the user to manually run the P2P application. The CloudCast system includes the b3d Installer, an ActiveX component that allows an* [sic] *web site that the user visits to instantly take advantage of the available P2P services. Approx. 40M P2P-connected users (approx. 15% of the active world-wide internet population) have the b3d Installer present on their machines, providing potential customers and partners with a massive group they can immediately reach. The b3d seamless-installation technology allows this user base to be reached even for new and previously unreleased applications, effectively future-proofing the existing KaZaA user base.'*

216 Counsel also referred to an Altnet document dated 11 November 2002 called 'Altnet Phase 2: Technical Description' ('the Altnet Phase 2 document') which described 'the software that Altnet intends shipping with Kazaa starting January 2003'. The software included the Altnet Download Manager which was said to have the following features:

> *'□ Download Manager is an ActiveX control that allows web pages to connect to the P2P stack.*
> *• Download Manager is also used by the Dashboard to download its instruction list, download resource-sharing files, etc.*
> *• Download Manager allows Altnet to sell TopSearch content into web sites as well as into Kazaa.'*

Counsel argued these two Altnet documents 'indicate a significant remote capacity in the TopSearch functionality which has not been explained away by evidence from any person on behalf of Altnet or BDE.'

217 Counsel for the applicants observed, correctly I think, that 'it is common ground that the Kazaa software supplied to new users contains a hard-wired list of IP addresses'. They said that, 'when a new user downloads the Kazaa program, the software attempts to communicate with at least one of those addresses'. Counsel then argued:

> *'it is essential for the effective operation of the software that the new user makes contact with a live supernode IP address on installation. The computer at such a live supernode IP address provides the new user with an updated list of supernode addresses and the new user connects with its relevant supernode. There is evidence that on the assumption the system is self-organising, a supernode's existence may be shortlived or not continuous. There is also the earlier evidence that some IP addresses can change ... The prospect that a commercial enterprise would leave to chance the possibility of one of those hard-wired IP addresses still being a current supernode in circumstances where a live address was critical to the useability of the software by the new acquirer and having regard to the volatility of an ordinary supernode's life, must be nil.'* (footnotes omitted)

218 Counsel argued this conclusion supported an inference of the existence of a central server. They said:

> *'The API indicates that there is a capacity in the recipient of the API, i.e. Sharman, to force a computer to be and remain a supernode. The clear inference is that someone, the obvious candidate being Sharman, is controlling one or more supernodes to ensure that one of the*

hardwired IP addresses will permit a new user to connect to the system. ... It being concluded that that prospect is not in fact left to chance but is controlled, the ready conclusion is that there is a central server.'

219 Counsel for the Sharman respondents argued there was no evidence of the existence of a central server, in the relevant sense of that term. In their Closing Submissions, they said:

'Once a user installs KMD, Sharman's ongoing interaction with the user is limited to the following:

(a) display of content from the Kazaa website on pages of the GUI;
(b) invitations to the user to upgrade to new versions of KMD; and

(c) receiving "bug" reports from users and referring them to the Kazaa website for assistance.

Other entities have ongoing relationships with users as follows:

(a) Akamai Technologies, which hosts the Kazaa website, has the ability to know the IP address, country and version of KMD pertaining to users;
(b) Altnet receives limited statistics regarding successful TopSearch searches and downloads; and
(c) third-party advertisers send advertisements to appear in the GUI, either as "banner ads" or "pop-up ads".'

220 Counsel also said that, if there were a Kazaa central server, 'it would be one of the largest concentrations of computing power on the planet'. Counsel asserted there would be 'immense problems of scalability and exposure to denial of service attacks'. They cited affidavit evidence in support of those assertions. However, the cited passages do not sustain the assertion. The passages merely make the point that peer-to-peer technology reduces the problems of scalability and service denial. Nobody has argued that a consequence of there being a Kazaa central server would be that all file-sharing traffic would be routed through that server. Altnet is an example of a system that combines a central server (TopSearch) with provision of music files from other sources. No evidence suggests there would be a problem of scalability or service denial if Kazaa was organised in the same way.

221 Counsel for the Altnet respondents submitted there are only 'three points of contact between Sharman and a user'. They were:

'(a) on the initial download and installation of the KMD;
(b) on the execution of the KMD;
(c) upon uninstalling the KMD.'

222 The initial download and installation is effected on Sharman's behalf by Akamai. On execution, the user sees advertising and promotional material sourced from Sharman's website, as well as some advertising material sourced from elsewhere. On uninstalling Kazaa, the user is given the option of providing a comment to Sharman.

223 Professor Sterling said that, other than these three contacts, 'there was no obvious communication to Sharman that he "could see in the code"'. He was assuming that the source code produced for his inspection was the source code currently used in the Kazaa system. This was not proved to be so. However, if Professor Sterling's assumption was correct, his evidence tends to negative the existence of a Kazaa central server.

224 The arguments of the applicants on this issue have force, especially in the absence of evidence confirming that the source code seen by some of the expert witnesses was identical to that actually used by Sharman. Moreover, no evidence was called from anybody who had been involved in the design of the system, such as Mr Kasesula. That would not have been because of the cost of bringing a foreign witness to Australia. Evidence could have been taken by videolink. Anyway, the Sharman respondents were prepared to spare no expense. They brought two experts out from America. Although one of those experts, Professor Tygar, made a commendable effort to understand the system, without being certain that it corresponded with what he understood to be the source code, it would have been preferable to have had an explanation of the system from one of the people who devised it.

225 On the other hand, Mr Morle (who should know) insisted there was no Kazaa central server. In some respects, I was not favourably impressed with Mr Morle. He tended to prevaricate and spar with counsel. He claimed total ignorance about matters of which he must have had some knowledge, such as Sharman's financial and administrative affairs. If he is to be believed, he had an astonishing lack of curiosity about the source and authenticity of the dynamic user figures that continuously appear on the Kazaa website. Yet I hesitate to conclude Mr Morle told a deliberate lie – it would have had to be that – about such a fundamental matter as the non-existence of a central server. This was an important matter directly within his area of responsibility.

226 The two American experts called by counsel for the Sharman respondents were Keith Wimberly Ross and Justin Douglas Tygar.

227 Professor Ross is Professor of Computer Science at the Polytechnic University in Brooklyn, New York. He has taught computer systems engineering at university level since 1985 and has published widely. At the time of giving evidence, he was researching aspects of peer-to-peer networking pursuant to three grants provided by the National Science Foundation, a United States government agency. The professor was obviously well qualified to give expert evidence in this case. However, my confidence in him was shaken during the course of his cross-examination.

228 Mr Bannon showed Professor Ross a draft of his report that contained a passage dealing with the relationship between Joltid's PeerEnabler software (used in FastTrack) and Altnet's TopSearch technology. The draft shows exchanges between Professor Ross and a solicitor at Clayton Utz, acting for the Sharman respondents. Professor Ross initially wrote the words: 'The Altnet TopSearch Index works in conjunction with the Joltid PeerEnabler to search for Gold Files'. The solicitor crossed out this sentence on the draft and suggested a substitute sentence: 'TopSearch searches its own Index file of available Altnet content and PeerEnabler is not needed or used for this, other than to assist in the periodic downloading of these indexes of available content'. Professor Ross replied: 'I was not aware of this, even after our testing. But if you say it is so, then fine by me'. He left the solicitor's words in the draft.

229 When Mr Bannon asked about this, Professor Ross responded:

> *'Unfortunately, I don't have the report memorised. But it is my recollection that I was not*

comfortable with this and I took it out in the end. But I would like to see my report to confirm that.'

230 Mr Bannon then showed Professor Ross the email showing the solicitor's response to his 'fine by me' reaction. The solicitor said: 'Keith, we want to try to avoid you being exposed to criticism so how about'. The solicitor then suggested the sentence that appears in Professor Ross' final report. The cross-examination went on:

'You see it wasn't you feeling uncomfortable. Clayton Utz said, well, in effect, Keith we want to try and avoid you being exposed to criticism, so how about something different. And they ruled out what you were otherwise prepared to swear up to based solely on their say so? --- I wouldn't agree with that. I wouldn't have been comfortable putting it into the final report I suppose unless I was given further evidence of this fact.

That is not what you communicated? --- Well you have to read between the lines. I said that we had phone calls as well and during the phone conversations often I would indicate that there were some things I was uncertain with and I would want an additional explanation or justification.

You said: "If you say it is so then fine with me." That is all you said? --- Once again I do not have my final report in front of me so I am not 100 per cent sure what I put there. But again in saying this I just know the way I am personally. What I am saying there: "Fine with me, once you give me additional proof".'

231 I cannot accept that explanation. I am forced to conclude that Professor Ross was prepared seriously to compromise his independence and intellectual integrity. After this evidence, I formed the view it might be unsafe to rely upon Professor Ross in relation to any controversial matter. Of course, that does not mean his evidence should be totally disregarded.

232 Professor Tygar seemed a more reliable witness. He is Professor of Computer Science and Information Management in the Department of Electrical Engineering and Computer Science at the University of California, Berkeley. He obtained a doctorate from Harvard University in 1986 and has taught computer science since that time. Professor Tygar has consulted for both industry and government, been a member of some government committees concerned with computer science and published widely.

233 Both Professor Ross and Professor Tygar asserted there was no Kazaa central server. For the reason I have indicated, I am not prepared to place much weight on this aspect of Professor Ross' evidence. However, I was impressed with Professor Tygar. He not only has excellent credentials; he had done his best to understand the Kazaa system, including studying the relevant part of what he understood to be its source code. Professor Tygar seemed to be attempting to assist the Court. He was aware of the central server issue, and its importance, and expressed a considered opinion about it. It is true, as the applicants emphasised, that it is not clear that Professor Tygar has had access to all relevant portions of the Kazaa source code; or even that what he was given was the source code actually used in the Kazaa system. However, Professor Tygar has spent much time examining the operation of that system. He is familiar with Kazaa's American counterparts. Under those circumstances, and especially as none of the applicants' experts was able conclusively to demonstrate the incorrectness of Professor Tygar's opinion, I am not prepared to find he is wrong in concluding that the Kazaa system has no central server.

234 There may be other explanations of the points raised by the applicants. There is room for doubt as to the true meaning of the API passages relied on by the applicants. Alternatively, as constructed, the Kazaa system may not have been conformed to the structure suggested by that document. Another possibility is that the system was modified after construction to remove the central server. The dynamic screen numbers of online users may be obtained in some unexplained way, but without use of a central server. The numbers may be estimates or simply made up. There may be a limited number of continuously-operating supernodes that supply IP addresses to new users.

235 There is no doubt that TopSearch is capable of monitoring and controlling the conduct of Kazaa users in relation to gold files. TopSearch is a central server, in the relevant sense, but (at the present time) only in respect of gold files. Although there is reason to suspect that there is, indeed, a Kazaa server that is capable of doing the same thing in relation to blue files, I am not prepared to make a finding to that effect.

(b) The range of indirect controls

236 However, counsel for the applicants argue that, even if there is no such central server, other measures were available to the respondents, but not put in place, that would have prevented (or at least limited) infringements of their clients' copyrights by Kazaa users. These were summarised in a document (exhibit L) prepared by the applicants' technical witnesses as follows:

*'**Filters***

1. The system could have been adapted and could be adapted to include non-optional filters which exclude the display in search results of Blue Files (but not Gold Files):

(a) with .mp3 file extensions; or

(b) any metadata of which matches a list of regularly updated keywords associated with artists and song titles in the Applicants' catalogues of sound recordings; or
(c) any metadata of which matches a list of regularly updated file hashes of versions of sound recordings in the Applicants' catalogues of sound recordings; or

(d) Boolean combinations of the above.

2. If there existed any authorized or public domain material the distribution of which would be prevented by any such filters of the type referred to in the preceding paragraph, such material could be distributed as Gold Files.

"Don't Share" Flag

3. The Respondents could have caused and could cause the setting of "don't share" flags to Blue Files identified as mp3 copies of sound recordings in the Applicants' catalogues which would have the effect of preventing the sharing of those files.

Monitoring

4. The system has a present capability of collecting and causing to be forwarded statistics and information in respect of individual users, including:

(a) username, user password and realms;
(b) IP addresses and country codes;
(c) file names;
(d) file hash values;
(e) metadata about files including title, author and keywords;
(f) content stored in individual files in "My Shared Folders";
(g) search results.

5. The Respondents could have regularly monitored and could regularly monitor individual Kazaa users' My Shared Folders to identify mp3 copies of sound recordings in the Applicants' catalogues.' (footnotes omitted)

I will discuss these possibilities, although not in that order.

(c) Monitoring of Kazaa users' files

237 Tom Mizzone is Vice President, Data Services, of MediaSentry Inc ('MediaSentry'), a company based in New York that provides online anti-piracy services. He heads a department that uses a platform known as 'MediaTarget' to collect information from computers. He has worked with colleagues to develop 'techniques to scan for, detect, and download copies of copyrighted material on multiple network protocols for use by copyright owners'. He said MediaSentry's technology 'tracks many popular distribution mediums including P2P networks ... using sophisticated scanning and detection software, to locate files that are suspected of infringing the rights of copyright owners'.

238 Mr Mizzone came from America to give evidence in this case on behalf of the applicants. In doing so, he was concerned to maintain the confidentiality of many of his employer's documents. He produced some manuals as confidential exhibits. However, in open affidavit evidence, he said:

'MediaSentry searches peer-to-peer networks for individuals whose computers are sharing type[s] of files with other users, such as music files and movie files. In the case of users of the Kazaa Media Desktop program, these are users who are sharing files from their computer, usually from a designated shared folder. These searches are undertaken for only publicly available files, being files that can be accessed and downloaded by any other user of the relevant system.

MediaSentry uses the same core technical processes that are used by peer-to-peer users to identify users. MediaSentry does not do anything that any user of a peer-to-peer network cannot do and does not obtain any information that is not available to anyone who logs onto a peer-to-peer network as a user.

When MediaSentry searches for music files on the peer-to-peer network, it views the files that each P2P user is disseminating to others, it obtains the IP address and screen name of each user, and downloads a selection of files offered by each user. These are all functionalities that

are built into the peer-to-peer protocols for the relevant peer-to-peer service, including the Kazaa Media Desktop, whether or not this information is always visible to a user in their specific peer-to-peer program.

In view of the potentially vast numbers of users of peer-to-peer networks, MediaSentry uses additional criteria to identify users with music files. It does this by using software that lexically compares the titles of the music files being shared on other users' computers with lists of music titles provided to MediaSentry by copyright owners.

When files are being downloaded, MediaSentry makes a record of the IP address used by the source computer. The process of downloading files from another computer involves the transmission to the receiving computer of information from the source computer such as the user's screen name (an alias chosen by the user, such as "Name@KaZaA") and the IP (Internet Protocol) address of the user. An IP address is a number that, along with the date and time, can be used to identify a computer using the Internet at the time.

Once connected to the user's computer, MediaSentry seeks to determine what other files the individual is offering to others for download. Kazaa and other file-copying programs permit users to share all of the files in their "share" folders, and they contain a feature that permits users to browse the entire share folder of another user. MediaSentry invokes this feature of the P2P program and is able to determine whether the individual user is offering for download one or more files and information about them.

Using a feature of the peer-to-peer software, MediaSentry captures a list of all of the files that the user is offering to share. MediaSentry collects this information in two forms. First, MediaSentry takes screen shots, which are actual pictures of the screens that MediaSentry or any other user of the peer-to-peer network can see when reviewing the files being offered. Second, MediaSentry creates a text file that includes all of the information on the screen shots, such as the names of each file and the size of each file, as well as additional information (called "metadata") about each file. Metadata may include a wide range of information about a file. Metadata, for example, can include information that identifies a person who originally copied the file or was the source of a file.

Once MediaSentry has the list of files being offered, it searches the list of files for copyrighted works owned by the record companies. Files offered by peer-to-peer users generally specify the name and artist of the song being disseminated, as well as the file type ("audio" for most music files) so it is relatively simple to identify files that are likely to be copyrighted sound recordings. In most cases involving peer-to-peer users offering hundreds or thousands of files for download, this search process uncovers substantial numbers of files that appear to be sound recordings whose copyrights are owned by the applicants.

Once MediaSentry has found a user offering files that appear to be music files owned by recordings companies, or that can be matched with a list of music files, MediaSentry downloads (as any other peer-to-peer user could) examples of them as complete files. They are then stored on MediaSentry's computer equipment.

At the end of its evidence gathering with respect to any individual user, MediaSentry has

usually gathered the following:

> *(a) individual audio files that appear to be copyrighted sound recordings that the individual is disseminating unlawfully;*
>
> *(b) a user log identifying all of the files that the individual was offering for download, as well as metadata about each of the files being offered;*
>
> *(c) screen shots of the user's share directory that show the files the individual was offering for download; and*
>
> *(d) the IP address, date, and time of the infringement, as well as the alias chosen by the individual (the user name) when participating in the peer-to-peer network.*

...

The gathered information can then be reported to copyright owners.

MediaSentry's process has multiple fail safes to ensure that the information gathered is accurate, including numerous steps to check and double-check the IP address of the potential infringer to prevent misidentification. MediaSentry also undertakes substantial and frequent audits to make certain that all of its systems are functioning correctly.

MediaSentry is not a subject matter expert on any music files identified with a peer-to-peer user and downloaded and therefore does not evaluate whether the files that it downloads are sound recordings whose copyrights are owned by record companies.'

On two occasions, in 2003 and 2004, MediaSentry carried out an investigation of this nature in relation to Australian KMD users.

239 In oral evidence, Mr Mizzone said MediaSentry had 500-600 scanners deployed. The scanners can search the FastTrack network to find those that have Kazaa loading. He said: 'We use a technique called subclassing to control the Kazaa application without a human needing to be in front of the computer'. His evidence went on:

> *'How do you know you're dealing with for example an Australian user? --- The results that we get back from the Kazaa application when we do search, the application itself provides us with an IP address of the end-user that had what appears to be the infringing material. We then do a "look up" of that IP address against a data base, in this case would be apnet.org which is the Asia Pacific network information centre. There would be authoritative body of IP address allocation in this area and to the extent that it is an IP address that has been assigned to a service provider in Australia we consider that user to be located in Australia.*
>
> *What's the mechanism by which you can identify the IP address of the user's file you're looking at? Is it some sort of signal which goes down the line and bounces back or what is it? --- Sure. We have a few steps and a couple of double-checks in which we do. At this level though the initial search we get that IP address from a file that Kazaa deposits on our scanners' hard*

drive. It's called a DAT file. That DAT file contains specific information about the user that responded to the search. Information such as IP address of the user core in which we're communicating with that user on file checks on metadata related to the file. All that gets stored in the data base. At that point we run the "look up" on that IP.'

240 Before commencement of cross-examination, I asked Mr Mizzone to confirm my understanding of his evidence in chief.

'Mr Mizzone, I want to take you back to what Mr Bannon asked you, ... just to make sure I am understanding what you say. I understand that you have got a big operation. But am I right in thinking that effectively what you do, although in an automated multi-machine environment, is to do what a person can do on a single computer; is that what you claim? --- That is correct.

And that involves, you go into the Kazaa system and you can identify a person who is using their computer, having logged into the Kazaa system, in connection with a particular file which is on a list you have been supplied by a client? --- That's correct.

I gather you can only pick them up if they are actually using it at that moment? --- That's right.

If they used it ten minutes ago and closed down the computer you wouldn't be able to find that out, you wouldn't be able to ascertain that they had swapped that file ten minutes earlier or played the file? --- That's correct.

So what you are doing is, you are in effect spying on a person who is in the act of downloading, is that what enables you to pick it up? --- We look for people that are sharing or distributing, we do a search for a file, the results that come back to us are individuals that have that file and a share directory, making it available for downloads.

Well, I gather if they have it in their My Shared File, you could get access to it in the same way as any other Kazaa user could get access to it? --- That's correct.

But your ordinary Kazaa user wouldn't know which node they were accessing at that time? --- That's correct, although there are ways in which you can see which IP addresses are connected to your computer.

Yes, explain that? --- Most operating systems allow you to run a command and NetStat is one of them, where you could at any time see the IP addresses which are connected to your system.

Are you saying an ordinary user could do that? --- Sure.

Well, perhaps not an ordinary user, because no doubt there are vast levels, different levels of sophistication, but ordinary equipment would allow you to identify the IP user address, is that what you are saying? --- That's correct, and the Kazaa application as you start a download puts a file in your share directory, the downloader share directory which contains the remote user's IP as well.'

241 Mr Mizzone claimed his company had technology to avoid decoys (false leads) and spoofs (icons that

never begin to download or transmit).

242 Cross-examining counsel did not challenge Mr Mizzone's account of his company's activities, although they did obtain concessions of the importance of the company's technology in being able to operate on this scale. Mr Mizzone agreed his computers would only pick up a shared file that used the name given to him by his client record company. He also agreed it would not be possible to connect to a user who had a firewall in place. There were also other steps a user might take that would impede the gathering of information.

243 Mr S G Finch SC, senior counsel for the Altnet respondents, led Mr Mizzone to speak of the specialised nature of his software and asked: 'You wouldn't be happy just to give it to us, would you?' Mr Mizzone replied: 'I would prefer not to'. Mr Finch responded: 'All right. We won't negotiate a fee in open court'. He then went to another subject, leaving unresolved the question whether MediaSentry might, for a fee, license the use of its software by others.

244 From a comment made by Professor Ross in an email to Clayton Utz, it seems he is engaged in research similar to the work done by MediaSentry. Professor Ross did not dispute Mr Mizzone's evidence. Particularly in that situation, I see no reason not to accept the evidence. However, it is necessary to remember that the information his company was able to gather was the result of an intensive (and no doubt costly) operation using highly sophisticated equipment.

(d) User identification system

245 Counsel for the applicants also argued the respondents could have taken steps to ensure they would be able to enforce the licence conditions in relation to copyright infringement. Counsel submitted:

> *'For example, new users could have been obliged to provide details such as name, residential address, email address and home and work telephone numbers. In addition, details such as the location of the computer on which the software was being installed including the owner of the computer and whether it was used as part of a business and if so the name of the business. ... there is no reasonable basis for assuming that a majority or even a substantial number of Kazaa users would provide false information on registration.*
>
> *Another aspect of this is that by default "all incoming instant messages" are blocked.*
>
> *The evidence suggests that Altnet has installed unique machine IDs in each Kazaa user's computer ... To the extent that that is not so, a machine ID could have been installed by the Respondents in each user's computer. In that way, personal details could be associated with identified activity in relation to that machine.*
>
> *Further, rather than give users the option of preventing searches of other files in their My Shared Folder, users could have been informed that monitoring of My Shared Folders for the purposes of ensuring compliance with the licence conditions was a right which Sharman reserved and would exercise. Ensuring that the instant messaging facility could not be blocked by users could also have been an aspect of the system provided by the Respondents.*
>
> *The removal of the veil of anonymity is likely to have a dramatic impact on unauthorised music file creation and exchange.'* (footnotes omitted)

246 As counsel explained, instant messaging is a facility that enables contact with a Kazaa user; making the facility optional allows the user to prevent that contact and so reduces Kazaa's control.

247 In their joint response to the applicants' technical experts (exhibit S3), Professor Tygar and Professor Ross said:

> *'The Kazaa UI has no capability of collecting and causing to be forwarded to Respondents statistics and information about individual KMD users. Although the KazaaLib API document contains information suggesting that user information could be provided to a central server, no evidence exists that such function or necessary hardware exists. To the contrary, evidence shows that no central server for collecting user information exists. Furthermore, there is no evidence that, even if a server for collecting user information existed, that information contained in subparagraphs (c) through (g) would be passed to a central server.'*

248 Professor Sterling was asked about a requirement for user identification. He thought it to be a possibility but he said he had not done the research about technical issues necessary to determine whether it was truly practicable. He said it would involve some redesign of the software.

249 Having regard to the technical evidence, I am not able to conclude it would be practicable for Sharman, in the absence of a central server, to implement a satisfactory system of obtaining particulars of users' identities.

(e) Termination

250 The Kazaa's website states:

> *'All users should understand that KaZaA has a no-tolerance policy with respect to child pornography and other obscene material. If at any time, KaZaA finds that you are using KaZaA to collect or distribute child pornography or other obscene material, [KaZaA] reserves the right to permanently bar you and your computers from accessing KaZaA and other KaZaA services. You agree that any termination may be without prior notice, and acknowledge and agree that we may immediately deactivate or delete your KaZaA account and all related information and files, and/or bar any further access to such files.'*

251 This policy assumes that Sharman is able to monitor a user's use of Kazaa and disconnect a user who offends the policy. Counsel for the applicants ask, if this is possible, why is it not possible to take the same action in relation to users who contravene copyright? They also point to cl 6.4 of the Joltid Licence agreement (see paras 102-106 above) concerning the effect of termination of the licence granted by Joltid to Sharman. That clause provided:

> *'Following termination of Licensee's rights to the Licensed Software, if ever, Licensee shall promptly discontinue the use of the Licensed Software and, at Joltid's instruction, given in the exercise of Joltid's sole discretion, shall, or shall permit Joltid to, deactivate, return, overwrite, and/or delete the Licensed Software and Joltid Confidential Information then in its possession and eliminate the ability of End Users to download additional Content using the Licensed Software. In addition, Licensee agrees that following termination of Licensee's rights to the Licensed Software, if ever, Joltid may through means available to Joltid, including by accessing the Licensed Software remotely or otherwise. (1) disable in whole or in part the Licensed*

Software and/or (2) prevent Licensee from using the Licensed Software to communicate with any or all End Users, and/or (3) prevent End Users from downloading additional Content via the Licensed Software, and/or disseminate any Update, or otherwise supplement, modify, render inoperable, or alter in any way the Licensed Software.'

252 As counsel observed, this clause is 'consistent with the view that the Kazaa software has a remote termination capability'. The clause suggests means of forcing an update on a user. It provides support for the suspicion that there is a central Kazaa server. However, having regard to other evidence relevant to that issue, I remain unprepared to find that such a server exists; in which case the threat of termination of pornography sharers' access is an empty threat incapable of fulfilment. Moreover, to the extent that it is impossible to monitor users' use and to force user identification, Sharman would lack the information necessary to implement a policy of termination for infringement of copyright.

253 Nobody has offered an explanation of the apparent inconsistency between the non-existence of a central server and the terms of cl 6.4 of the Joltid Licence Agreement. Once again, I mention the possibility that, at one time, there was a central server, or at least a proposal for a central server, but the situation later changed.

(f) Keyword filtering

254 Counsel for the applicants suggested that the respondents could have designed non-optional filters which would prevent the display of search results of blue files whose particulars (title, artist etc) matched particulars of the sound recordings listed in the applicants' catalogues. Counsel said such a filter could have been designed to be independent of any filter associated with gold files and to be capable of remote activation by the respondents.

255 Mr Morle discussed the possible use of filters in his main affidavit. He said:

'I am aware that KMD can identify Altnet files as gold icons because it obtains the Altnet results independently from the FastTrack results. This is not a filtering process. The KMD cannot filter unauthorised copyrighted files while allowing the searching and downloading of non-copyrighted or licensed files. I am not aware of any technology that could perform this function.

The KMD contains two simple filters – namely:

22.1 One filter allows a user to block any executable file (i.e., a file with a ".exe" file extension.

This can be set by a user concerned about possible viruses in executable files; and

22.2 a second filter, called the adult filter, blocks the display of files that contain in their metadata certain words that are sexually-oriented or offensive.

This filter can be set in the "No Filter", "Offensive Content", "Adult Content" (Default) or "Images and Videos" position, and can be password-protected by parents.

To my knowledge the Respondents do not have, nor are they aware of, technology that would filter content owned by persons such as the Applicants, while allowing the search and download of other content.'

Mr Morle said he understood some discussion about this matter had occurred in America. There is no evidence, either way, about that.

256 In cross-examination, Mr Morle agreed with Mr Bannon that measures to control the distribution of blue files would not affect the distribution of gold files. Mr Morle told Mr Bannon he had discussed filters with Ms Hemming. However, no steps in that direction ever were taken. Mr Morle gave this evidence:

'You see, what I want to suggest to you is that you have never participated in any executive decision by Sharman, to take any step to admonish or criticise any individual user or group of Kazaa users for infringing the applicant's sound recording copyright using the Kazaa system, have you? --- I don't think I have personally. I am not aware of anything else that has occurred.

And you can't point to a single piece of paper which describes any campaign or communication to the public or to users, leaving aside the initial documents under the initial agreement which constitutes any campaign to persuade users who you believe are infringing copyright using the Kazaa system to stop doing it. That's right, isn't it? --- I can't think of anything beyond the warnings that are around the website.

...

You have never taken a single, solitary step to attempt to introduce filters which would inhibit infringement in the applicant's sound recordings, have you? --- I've spent a lot of time thinking about filtering and considering how that would be done and I haven't got to a position where what I've reported can and can't be done has caused my superiors to want to try anything.'

Mr Morle said his reports on filters had been given 'verbally'. He was unable to point to any written report.

257 Mr Morle agreed the Kazaa system incorporated 'advanced searches' limiting search results to particular categories of files: audio, video, software, archives and play lists. He did not agree those searches were filters but he accepted their effect was to limit the material a user could download. Mr Morle said there was an 'adult' filter and a 'custom' (common word) filter.

258 Mr Morle also agreed that Mr Morris had told a United States Senate committee that Sharman had 'the most comprehensive' adult filter and monitored for child pornography. However, Mr Morle said he did not know how Sharman could prevent the Kazaa system being used for this purpose.

259 I do not accept Mr Morle's evidence about discussing filters with Ms Hemming, at least in any serious way. Mr Morle's evidence was not, of course, confirmed by Ms Hemming. Although she attended much of the trial, she preferred the well of the court to the witness box.

260 The documents tendered in evidence demonstrate that Mr Morle extensively used email to communicate with his colleagues, including Ms Hemming, even on subjects of minor importance. I find it difficult to believe he would not have used email to communicate any significant views on a matter as important as the

introduction of blue file filters. Moreover, although Mr Morle posed as financially unaware, he is neither stupid nor commercially inexperienced. It would have been obvious to him that it was not in Sharman's interest to impede sharing of blue files. The focus groups showed the primary purpose of most Kazaa users was to obtain free access to music files. Free access was available only from the blue files. A filter that impeded, or significantly curtailed, blue file sharing of popular music would have seriously diminished Kazaa's appeal to users and, therefore, the number of people using it at any particular time. That would have adversely affected Kazaa's appeal to advertisers.

261 The fact that I reject Mr Morle's evidence on this point, and that no other Sharman or Altnet employee gave evidence about it, does not mean blue file filtering was a realistic proposition. There was expert evidence about this topic.

262 In an affidavit read at the trial, Professor Sterling said 'there are a number of measures that could have been taken by the developers of the software in order to filter or attempt to exclude unauthorised material from the system and from KMD users'. He explained:

> *'The Guide describes the existing ability of KMD to filter in at least two circumstances. One circumstance is for protection against viruses by removing files with suspicious extensions such as .scr or .bat. From the perspective of the design of the system, it would be no harder to screen files which have a .mp3 extension, even if the existing filter technology is deployed.*
>
> *The second circumstance is the existing KMD filter for adult content, that looks through metadata such as the file title. The Guide refers to this filter being used to block material that is offensive and inappropriate for children is blocked.*
>
> *In my view, it would be equally possible to filter out files because of copyright content. Consider the band Powderfinger ... In my view it would be straight forward not to allow any files with "Powderfinger" in the title metadata. While filtering in this manner may not always be accurate, such that the file that is filtered may not actually be by Powderfinger, or alternatively all Powderfinger files may not be removed, the filtering by metadata is likely to restrict the availability of files that are correctly labelled as being Powderfinger files.*
>
> *Given that such files would ordinarily be searched for by name or metadata that referred to Powderfinger (or some other known data) and KMD users appear to be rewarded for correctly labelling files (in the Glossary to the Guide) I would expect that even this simple key word filter would be likely to restrict unauthorised Powderfinger files.*
>
> *An analogy can be drawn with Spam filters for e-mail. While it is impossible to block all spam it is a standard industry practice and one that is useful to provide partial solutions by keyword-based filters. Many email filter products ... are nothing more than that.*
>
> *Another means by which unauthorised files could be filtered for KMD users is by use of file hashing identification processes. I am aware from Mr Thompson's report that KMD uses file hashing technology.'*

David Erskine Thompson is an expert in computer forensic technology who gave evidence on behalf of the applicants.

263 Before Professor Sterling was cross-examined at the trial, I directed his attention to the technical experts' agreed propositions (exhibit G), to which he was a party: see para 129 above. I asked him about para 10 of the document, dealing with non-optional keyword filters. He said the reason for the qualification in subpara (e) was that it was not possible to guarantee that people would not try to find ways of overriding the filter; for example, by giving a particular singer a nickname. In relation to subpara (f), Professor Sterling said that, if he wanted to distribute his own work under the name 'Leon Sterling', and there happened to be a popular artist of that name, he might be blocked regardless of his wishes. I asked Professor Sterling whether there was an answer to that problem. He replied:

> *'To solve it in generality, no. I think this was a kind of agreement, the level of effectiveness of such filters is certainly something which I think is perhaps to some degree in dispute'.*

264 Under cross-examination by Mr Leeming, Professor Sterling agreed there was no 'answer in the sense of a 100 per cent effective filter that has no false negatives and no false positives'. Professor Sterling said 'some people might be able to get around' a filter, but he thought 'it actually would be effective for a large percentage of people'.

265 Mr Leeming drew Professor Sterling's attention to an earlier report he had prepared about Kazaa. In that report, Professor Sterling said that reading the Kazaa user guide had reinforced his previous perception that Kazaa 'was designed to have music files'. Under the heading 'Copyright protection', Professor Sterling had said:

> *'Users are encouraged to share files. There is some kind of rewards mentioned for people to share files. In the case of music files, there is nothing in the interface that suggests that users need to be careful of copyright violations. There are disclaimers at the bottom of the Web page with the user's guide, but not in a way that will make users take notice, or think about the copyright issue. In general, I had the impression that the warnings about being careful to observe copyright were buried in the guide. Given the publicity surrounding the Napster case, no developer should be unaware that copyright for a file-sharing application that facilitates sharing of music files is a key requirement to be handled properly.*
>
> *It is understandable that the developers of KaZaa would encourage users to share files. Certain applications, and KaZaa is one, are only useful if there is a sufficiently large amount of content available through it. People will use Kazaa rather than another program only if it is easier to use and give better results.'*

266 Mr Leeming referred Professor Sterling to what he had written in this report about filters:

> *'The authors state that it is impossible for them to filter unauthorised files. This claim is inaccurate and misleading. While deciding whether a file is authorised or not is probably technically impossible, there are certainly measures which could easily be taken.'*

267 Professor Sterling had referred to the fact that the Kazaa system provided for filtering against viruses and commented: 'It would be no harder to screen files which have a *.mp3* extension'. He also referred to filtering for adult content by looking through 'metadata such as the file title'. He said: 'It is hard to envisage that it is not equally possible to filter out files because of copyright content'. Professor Sterling told the hearing he continued to hold the opinions he had expressed in this earlier report.

268 Professor Sterling said there would be a number of design issues in establishing a filter system. He had not thought it his role to do the design work. Professor Sterling agreed there would need to be 'communication with the music industry' and 'a means of comparing the files that users have with the applicants' catalogue files'. As a general principle, he thought, it would be better to do that at supernodes rather than at users' nodes. The evidence went on:

> *'Do you agree with me, as presently implemented this filtering that you propose does not appear? --- Currently they are not filtering on these mechanisms.*
>
> *You would have to turn the present optional filters into non-option filters; so you would have to re-write? --- There would be some changes to the code necessary and I am not going to speculate on the degree of difficulty.*
>
> *And you would need to update those filters from time to time as well? --- Yes.*
>
> *...*
>
> *Dealing with existing users an initial question is whether or not there is an ability to force an update upon the user; a termination question as you have labelled it? --- I have commented on that previously. I don't have more to comment.*
>
> *I am not asking for your comments, Professor, I just want to know whether you agree that that is a threshold question that has to be addressed before we get to filtering in the case of existing users? --- Something needs to change in the existing user's program in order to apply these filters more effectively, absolutely.*
>
> *Thank you. The second thing about filtering, do you agree, is that whatever you do it is not going to be 100 per cent effective; is it? --- Yes, agreed. That is one of the overall requirements that needs to be taken into consideration.'*

269 Professor Sterling said he was not able to tell the Court, in any detail, what he meant in saying the Kazaa system could have been adapted, and could now be adapted, to include filters based on metadata matching a line of regularly updated file hashes**.**

270 Professor Sterling conceded to Mr Meagher that he had not undertaken any research 'to see whether or how filtering might operate in relation to a peer to peer application'.

271 In para 92 of his affidavit, Professor Tygar offered some comments about Professor Sterling's affidavit. At subpara (j) Professor Tygar said:

> *'[Professor Sterling] suggests that KMD could be modified to ban files having an MP3 extension. While this is certainly technically possible, it would ban all files marked with the MP3 extension, regardless of whether they were authorized for exchange or not. Such a ban would deny the many artists without record label contracts an important, alternative, distribution mechanism. ... Furthermore, it would not prevent users from exchanging files of the form* musicfile.txt *which were later manually converted to* musicfile.mp3. *Of course it would also not prevent users from exchanging audio files in any other format, some of which I have discussed above. ... Prof. Sterling further suggests filtering on band names such as*

"Powderfinger", although he readily concedes that those filters would yield both false positives and false negatives: "all Powderfinger files may not be removed" and that some removed files "may not actually be Powderfinger." Prof. Sterling fails to address the complexity in coming up with a list of all keywords relevant to copyrighted works (imagine the difficulty in deciding which recordings of Beethoven's Fifth Symphony are authorized for distribution) let alone distributing and keeping the list up to date. Finally Prof. Sterling makes an analogy with spam filters ... but he fails to address what most e-mail users know: that those filters are increasingly ineffective at stopping spam as clever spammers find new ways to avoid detection by the filters. Finally Prof. Sterling addresses the use of hash values as a way to filter files; but as I discuss above, these methods can only filter a specific representation of a specific music file, not all representations of all unauthorized music files.'

272 During his cross-examination of Professor Tygar, Mr Bannon did not challenge the professor's view about false positives and false negatives. However, he did ask Professor Tygar whether he was arguing that, if a filter 'can't be 100 percent, it shouldn't be implemented at all'. Professor Tygar responded:

'Well, I do think that some threshold of effectiveness ought to be met and that we should consider the question of filters in regard to how users would actually use them and deal with them in practice'

273 Mr Bannon put to Professor Tygar that 'a selection of hash value versions of a particular sound recording would have the potential to severely limit the extent of distribution of that sound recording'. Professor Tygar replied: 'For a while, yes, but not indefinitely'. He later explained: 'I could imagine such a system might be effective for a week or two'. The evidence went on:

'And the system could be adapted to change hash values? --- When you say the system, are you referring to KMD?

The filter? --- The filter. Indeed, you could receive updates but the phenomena that I was expecting was that users would download programmes which simply introduce random changes into a file, for example, random changes into what's called an ID3 Version 2 Header by adding some field to the comment, adding an additional set of random letter[s] to the comment, thus generating a nearly unbounded number of variants of an identical music recording that would yield different hash values.'

274 I asked Professor Tygar some general questions about methods of achieving a balance between copyright protection and freedom of information. The professor said he had given thought to this issue. His evidence proceeded:

'my own belief is that the best way to address these issues is through technology that keeps users from infringing copyright in that way and there's extremely rapid progress being made in this area. For example, Windows now offers WMA format files that have something called Digital Rights Management. The digital rights management system makes it very difficult for users to exchange those files infringing copyright. Broadcast material in the United States, [in] particular digital broadcast material, now has flags associated with it that restrict the ability of the receiver to do certain things with that information. Watermarking technology that's been developed can help assist in catching cases where infringement happens. I believe that the problem is so pervasive of copyright infringement in our society that legal mechanisms alone

can never address this.

...

But you can go to different technologies I suppose, totally different technologies, but I guess you can't force people to use them and if, in a particular case, it suits a commercial establishment to offer the MP3 technology then why would they abandon that in favour of different technology, whatever problems that might force upon them for the sake of cutting down on infringement? --- Of course it's the decision of the information owner and distributors how to present that information to society.

Yes? --- So ultimately the decision rests in their hands but regrettably the pattern that we see with the rapidly evolving technology is that even when sources of copyright infringement are shut down other sources are emerging very rapidly and the problem is an adaptive one, your Honour, as individuals face additional restrictions they change their behaviours. I worry that legislative or judicial decisions alone would not be sufficient to address the problem.'

275 Professor Ross also replied to the affidavit of Professor Sterling. He made the point that, by filtering on .mp3, all .mp3 would be blocked, including non-copyright files. He thought this 'clearly unacceptable for new artists who are looking to use P2P file sharing as a marketing tool'.

276 Professor Ross rejected Professor Sterling's comparison with filtering spam in email. He said:

'Blocking spam is more straightforward as a relatively small number of words will catch most of standard spam (solicitations for money, pornography, medical drugs, etc.). The list of words necessary to provide any kind of effective filter by reference to the metadata of shared files would be enormous and constantly changing. Someone would need to compile the list and keep it current. Given the vast quantity of material in which copyright might subsist (whether audio, text, image or movie files), it would be a mammoth ongoing undertaking to create a list that could filter unlicensed versions of such material that users choose to share. Further, users can control the metadata attaching to files and can easily change descriptions to avoid the filter.'

277 Professor Ross also disagreed with the possibility of using the file hash to filter unauthorised files. He said:

'... content can have tens of thousand[s] of versions, each will give a different hash function. Filtering with the content hash will not work well because there are many different versions (with different hashes), and different versions are being introduced every day.'

278 During the course of his cross-examination, Mr Bannon put to Professor Ross the possibility of using the gold file system to 'provide page after page of gold file responses, each of which said something like "don't infringe copyright" and actually didn't provide any content'. Professor Ross responded:

'Obviously you can write software so that if you type in some key words and what pops up is, "Do not infringe copyright law", yes, that can be designed'

279 Professor Ross rejected the idea of filtering particular hash versions. He said:

'I don't believe it would work at all, quite honestly. Take an example: suppose you have a file that has 10,000 versions. Suppose somehow you decide to have a filter that blocks out the first 5000 most popular versions. When the user goes ahead and does a search, there is still going to be - those other versions are still going to appear in the user interface. So the user can still go ahead and download the copyright and many many users, millions of users will be doing that and they will all be downloading it and then before you know it the version that had popularity 1000 is now popularity one.

Well, in other words you are saying yes, it will work for a while but you may have to change the system? --- I think it would work in the order of a half an hour or an hour.'

280 I think it is apparent that a hash filter system would be ineffective. It is also apparent – indeed common ground between the experts – that a keyword filter system that was tied to the title of the sound recording or the name of the artist would not be 100% effective. However, counsel for the applicants argued this was no reason to reject the view that the respondents could have used this technique substantially to inhibit copyright infringement. In their Closing Submissions, counsel said:

'The Kazaa system depends on file sharing. That in turn depends on millions of users communicating in the same language. The heart of the system is the search request and search results system. That system is word-based by reference to the metadata of the Blue Files. ... Sharman encourages users to be as accurate as possible in describing files and to correct file names when downloaded into My Shared Folders. That is an admission that the system requires accurate descriptions to be useful. There would be no point in a user deliberately misdescribing a file unless other users understood the "code". There is no evidence that a new code could be sensibly developed among users. Further, any such code could only work if it was universally known, in which case in [sic] *would necessarily become known to Sharman so that the new code word could be added to the filter.*

As previously indicated, the success of the system depends on maximising the number and location of users. If, as the evidence indicates, and as the Applicants contend, the success of the system depends on the sharing of unauthorised music files, making the system difficult or cumbersome in relation to such files would quickly lead to its demise. If the system was not so dependent, it would have no impact.

In any event, a concern that a filter may not be 100% effective is not a valid reason for not implementing it. The adult filter is thought worthwhile although it is not 100% effective. The same may be said about virus filters.'

281 Counsel also dealt with the false positives concern. They said:

'The other "concern" expressed in relation to such a filter is the prospect that it might exclude some authorised content. That concern appears to be speculative. For example, Professor Tygar could not proffer any specific example of any authorised content which would be excluded by such a filter. To similar effect was the evidence of Professor Sterling. Despite the efforts of the Respondents to produce evidence of actual use of KMD to distribute copyright-free content, analysis of the raft of affidavits they filed and read seeking to support that proposition shows that beyond the most generalised statements 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.

In any event, the Gold File system is available to ensure that any content which might conceivably be excluded by the Blue File word filter could be and could have been made available as a Gold File and hence not excluded by the Blue File filter. The evidence indicates that Altnet has offered exactly that service to the Creative Commons content providers. Moreover, the Respondents were eager to urge on the Court that all the material described in the affidavits of Prelinger, Kahle, O'Reilly, Newby and Fitzgerald was free of copyright claims. If they have satisfied themselves of that sufficiently to say it to this Court, then they must have satisfied themselves of it sufficiently to be confident in making the content available as Gold Files without fear of liability.

Finally, the mere risk that there may be some files excluded from the search results is not a reason why the filter should not have been implemented. The Respondents include a virus filter which excludes all .dll and .exe files. That would exclude many files which are not viruses. As the Court room demonstration showed, the adult filter excluded files which consisted of sound recordings by the Sex Pistols which would not be regarded as the type of adult content that is the object of the filter. Furthermore, the stated vision of the Respondents is that software be used by users to acquire Gold Files. Mr Morle himself said that limiting the sharing of Blue Files was not a matter which concerned the Respondents.' (Footnotes omitted)

282 In their Closing Submissions, counsel for the Sharman respondents argued there were four difficulties about filtering:

(i) making filters non-optional;
(ii) identifying what is licensed;
(iii) getting a list of metadata for licensed works to the user's computer:

> *'such a list would be long, it would take up a user's download bandwidth memory, and performance; very plausibly, the sites from which the list came would be the subject of hacker attacks and there would be other means of circumvention;'*

(iv) false positives:

> *'it is no part of the Applicants' statutory right to require a system (filtering or blocking technology) which suppresses the distribution of works or recordings in which they do not own copyright.'*

283 Counsel said, I think correctly, that '[t]here is no evidence of the existence of a non-optional filter, whether within the KMD or otherwise, where a third party determines the content to be filtered and imposes that on users. There is no evidence as to how such a filter could have been created and implemented'. They claimed three problems associated with such a filter:

> *'(i) if the filter resides on a user's computer, he or she has the power to remove or alter it;*
> *(ii) users could easily block the communication of updates of filter terms to the user's computer;*
> *(iii) there is no effective way to limit such filters, or indeed any filter, to particular*

jurisdictions such as Australia.' (footnotes omitted)

284 Counsel supported this submission by referring to exhibit S3, produced jointly by Professor Tygar and Professor Ross as a response to propositions advanced by some of the applicants' technical experts. In relation to keyword filtering, the two professors said this:

> *'(a) Determining whether to locate the filter in the Kazaa UI or the Kazaalib file. If placed in the Kazaa UI, significant performance problems would arise as each search result returned from the Kazaalib to the Kazaa UI would need to be compared to the filter list prior to display. Depending on the size of the filter file, this could significantly delay the display of search results. On the other hand, the Respondents have no ability to add a filter to the Kazaalib file themselves.*
>
> *(b) Preparing a list of files to be filtered.*
>
> *(c) Formulating an effective combination of terms.*
>
> *(d) Communicating the list to the Respondents to be provided to users.*
>
> *(e) Having enough users accept a new version of the KMD application with the filters so that it has any effect, since versions of KMD without the filter would continue functioning without interruption.*
>
> *(f) Updating the key word list in an effective manner: Even assuming a user downloaded a new version of KMD with filters, no effective way exists of ensuring necessary updates. Any location from which updates are provided could be blocked at the source or at the user's computer. For example, a user could block access to any website providing the updates through his or her firewall. Likewise, users could initiate denial of service attacks against such websites.*
>
> *(g) Preventing false positives: The experts accept that any filter will necessarily block public domain and authorized content. As one example, many bands allow the electronic distribution of recordings of their live performances.*
>
> *(h) Preventing circumvention. Many techniques exist to circumvent filter technology. In the context of file sharing technology, for example, Napster users devised means for avoiding the key word filter it implemented in less than 24 hours, including renaming of files, misspelling, and use of Pig Latin (these renaming procedures were quickly automated). These avoidance techniques proved so successful, that the record companies subsequently reported to the Court in that matter that virtually none of their copyrighted recordings were blocked from download. Moreover, any filter could be circumvented by deleting the key word file from the user's computer, or replacing the key word file with a "null" file. While there may be countermeasures to this, these measures may give rise to further difficulties.*
>
> *(i) Limiting to Australian users: There is no effective way that such a filter could be made specific to Australian users.'* (footnotes omitted)

The two professors also listed problems with file extension filtering and file icon filtering. It is unnecessary to set out those problems. Professor Sterling effectively conceded that neither of those techniques was feasible.

285 In cross-examination, Mr Bannon put to Professor Ross that he could 'conceive the possibility of designing filters which could filter out different adjustable keywords'. Professor Ross replied: 'Yes, in many of the documents I put forth you can include filters that filter out these words'. Mr Bannon then suggested the keywords could be made remotely adjustable. Professor Ross said: 'I think it would be a very difficult task to do that but it is possible, as outlined in my response to the applicants' experts.'

286 One argument in relation to keyword filtering may be immediately addressed. Counsel for the Sharman respondents said:

> *'There is no evidence that a list of copyright files exists, that such a list was ever made available to the Sharman Respondents or as to how such a list could be created without the co-operation of the Applicants or any other relevant copyright owner. While the Applicants have provided no particulars of the size of their catalogues, if their assertions as to the extent of those catalogues are to be accepted, clearly the size of the filter file would be enormous and constantly changing. Someone would need to compile the list and keep it current. Given the vast quantity of material in which copyright might subsist (whether audio, text, image or movie files), it would be practically impossible to create a list that could filter unlicensed versions of such material that users chose to share.'*

287 These assertions are correct. However, it is not significant that no list of copyright files presently exists. Having regard to the attitude of the respondents, the occasion for creation of such a list has not yet arisen. Of course, it would be necessary for the applicants, and other copyright owners, to co-operate in the creation of such a list. To the extent they refused or neglected to do so, they would deny themselves such copyright protection as keyword filtering might provide to them. It would also be necessary for the list regularly to be updated. This would be an onerous ongoing task. However, to the extent that copyright owners neglected to do this, it would be they (not the respondents) who would suffer.

288 It is convenient also to comment on the 'false positives' argument. 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. If that impression is incorrect, the respondents have themselves to blame. They could have put before me evidence as to users' searches. Users' searches are routinely monitored by TopSearch, in order to enable Altnet to offer gold files thought appropriate to the particular user's apparent area of interest.

289 During the course of the hearing, the Court was treated to a vivid example of a false positive arising out of the use of the adult filter. Counsel asked a witness to use Kazaa to call up a particular piece by the Sex Pistols band. The witness could not do so. Kazaa denied access, apparently because 'sex' was one of the words proscribed by the adult filter. Nobody argued the aberrant result of this search would require or justify abandonment of the adult filter.

290 I accept that some canny users would devise methods of evading a keyword filter; for example, by the

adoption of a nickname for the artist or a codeword for a particular song. However, this technique would allow file-sharing of the relevant works only as between people who were privy to the adopted nicknames or codewords.

291 In their joint document (exhibit S3) Professors Tygar and Ross spoke of the necessity to determine whether to locate the filter in the Kazaa UI or the Kazzlib file. That dilemma is not a valid argument against keyword filtering. If it would be reasonable to require the respondents to undertake keyword filtering, and their decision was to place the filter in the Kazaa UI, any slowing of the file-sharing function would be merely a consequence of the respondents carrying out their duty. If the respondents preferred to locate the filter mechanism in the KazaaLib file, they would need to do this by arrangement with Joltid. Having regard to cl 3.2 of the Joltid Licence Agreement, that should present no difficulty.

292 Counsel for the Sharman respondents contended that Professor Sterling 'conceded that filename filtering could easily be evaded'. I do not think he did; the relevant evidence is set out above. Professor Sterling merely conceded there would be false positives and false negatives. As in the case of the adult filter, perhaps this disadvantage should not be regarded as conclusive.

293 In their Closing Submissions, counsel for the Altnet respondents emphasised Professor Sterling's concessions and the inevitability of some false positives and false negatives. They spoke about the problem of getting a list of metadata to the user's computer; the list would be long and would occupy considerable download bandwidth, memory and performance. These are design issues. Professor Sterling did not pretend he had resolved them.

294 There are obvious difficulties about a system of keyword filtering. However, I am not persuaded it would have been beyond the ability of Sharman to overcome those difficulties. I accept any keyword filter will not be totally effective. I also accept it may sometimes produce false positives. However, the fact that a protection is imperfect is not a sufficient objection to its adoption. Even an imperfect filter would go far to protect copyright owners, provided they were prepared to go to the trouble of providing and updating a list of keywords (titles, performers etc).

(g) 'Persuaded' upgrades

295 Another argued problem about a requirement that the respondents (or some of them) take action to install keyword filtering is its difficulty in relation to existing users. If the Kazaa system included a central server that could manipulate existing users' software programs, there would be no problem. That is common ground. But I am not able to conclude the Kazaa system does include such a central server.

296 It is also common ground that, if keyword filtering is a reasonable requirement, it would be possible to impose that filter upon new Kazaa users. The software package supplied to new users could be made to include the necessary filtering elements. The problem arises in relation to existing users.

297 The reason for the problem is that, in the absence of a central server, it is not possible for the respondents (or any of them) directly to amend the software package that is already installed in users' computers. Keyword filtering can be made to apply to those users only by persuading them to install (that is, download) a new software package that contains the necessary filtering elements.

298 Although there is no evidence about numbers, it may be assumed many Kazaa users, who had previously installed a 2.6 version on their computers, elected to upgrade to a 3.0 version. That would have

been a simple process; they would merely have needed to press the appropriate click link to download KMD v3.0 or Kazaa Plus v3.0. Those who elected to upgrade were presumably motivated to do this by material on the Kazaa website extolling the virtues of v3.0. No doubt, they believed it would be to their advantage to install v3.0.

299 All parties accepted it would not be to the advantage of people who use Kazaa in order to obtain access to copyright material for them to install a new software program that included a keyword filtering mechanism. To the extent the filtering was effective, they would find themselves restricted. Why, then, would they agree to 'upgrade' to the new program?

300 All parties conducted the trial on the basis that most Kazaa users would be unmoved to upgrade to a more restrictive program by exhortations against copyright infringement, appeals to fairness and the like. [The fact that the respondents shared – indeed, emphasised – that view itself indicates their perception about the reason for users' interest in Kazaa.] All parties assumed it would be necessary to press users to upgrade. The applicants conceded it would be difficult to exert sufficient pressure; the respondents contended this would be impossible.

301 Although counsel for the applicants argued it would be possible to force existing users to upgrade – I will come to that – they contended this is not a critical issue. In their Closing Submissions, counsel said:

> *'It is no answer to the case for the Respondents to say that given the amount of software out in the marketplace without filters, it is too late for the Court to require that imposition now. It would simply mean that on the one hand they have authorised or committed many infringements, and on the other hand that they will be prevented from doing so in the future. This is so regardless of the auto update issue.'*

302 Turning to what they call 'auto update', counsel said:

> *'An issue in the proceedings has arisen as to whether there is a present capacity in the system to force whether by technical (or absolute) or by behavioural (or relative) means on existing users an update of the software which includes the filters. If the Respondents were precluded from supplying any further software to new users except software with the filters and from supplying any updates to any existing users other than updates which included the filters, existing users would be deprived of the benefit of any enhancements to the system including any bug fixes without accepting the filters.'*

303 This observation appears to be correct. However, many (possibly most) users might be prepared to bear that burden, rather than lose access to copyright material.

304 No doubt for this reason, counsel for the applicants went on to refer to evidence which, they said, 'indicates that there are practical means of forcing an update on users even if it is only by force of rendering the existing version impracticable to use by incessant update offers'. Mr Morle gave some evidence about this technique.

305 Mr Meagher showed Mr Morle an email (exhibit M) sent by one Sharman employee (Michal Hempel) to another (Mr del Re), dated 12 November 2003, concerning methods of persuading users to upgrade to later versions of Kazaa. The email was not written in the context of upgrading to a keyword filter system. The proposal, essentially, was the use of a Message Box ('MB'), controlled by Kazaa, which would

encourage users to upgrade. The messages would appear with increasing frequency. The MB would offer only an 'upgrade' button. Mr Hempel concluded: 'MB will not give the option to close and user will be compelled to upgrade'.

306 Mr Morle did not agree that a user would be compelled to upgrade. He said that, if the user did not press the 'upgrade' button, the old version would remain on the user's computer, 'the user would be able just to close that window and the whole process would stop'; this would not prevent the user using the Kazaa system.

307 When Mr Bannon cross-examined Mr Morle, he asked him further questions about exhibit M. Mr Bannon suggested to Mr Morle that it would be possible to 'drive the user mad with dialogue boxes until they've upgraded'. Mr Morle said 'we actually try and do that and there are many people that still do not upgrade'. After some technical discussion between Mr Bannon and Mr Morle, I sought to clarify Mr Morle's position. This exchange occurred:

> *'[C]ould the user enjoy the sharing facility until such time as it had satisfied the urgings of the upgrade button? --- Well, like I say, you couldn't just have an upgrade button, but assuming a dialogue box appearing on the screen repeatedly they would find it quite difficult.*
>
> *To use the technology, to use the sharing? --- If that's possible.*
>
> *So in other words what Mr Bannon, colourfully, calls driving them mad, they stop them in fact enjoying the sharing facility? --- Yes, I mean I can't say 100 percent that it will stop the user clicking on the application, but if that is the case it would certainly drive them mad. If that dialogue did lock them out of clicking the rest of the application it would drive them sufficiently mad, yes.'*

308 In response to Mr Meagher, Professor Tygar gave some evidence relevant to this matter. It was as follows:

> *'there has been some evidence given about the possibility of Sharman causing some pop-up box to appear on the view that the user of the KMD has which only offers the choice of installing an upgrade. So as to in effect force the user in some way, by repetition, or what-have-you, from doing anything other than installing the upgrade; is that possible? --- It is not possible.*
>
> *Could you explain, please, why? --- When people use the web it is often the case that certain web pages try to put up pop-up displays often these are advertising displays. There is ability within web pages and within pop-up messages in general to request that the user make a choice. However, it is always possible to disregard pop-ups. In fact, pop-ups have become so annoying that modern web browsers such as the version of Internet Explorer that's currently distributed by Microsoft or its most popular competitor, Firefox by default automatically block pop-ups. There is also third party software from companies as large as Google or as small as the company that distributes pop-up stock that will block pop-up blockers.*
>
> *Right? --- Statistics seem to indicate that these pop-up blockers are quite popular, so it is in fact not technically possible to foist a decision on a user by the user of pop-up boxes.*
>
> *Professor, one last question. Does KMD use the Microsoft Internet Explorer as its browser? ---*

It does. In fact it requires Microsoft Internet Explorer.'

309 The question whether Sharman could control the operations of the browser was not explored by counsel. In the absence of specific evidence on the point, and because of my inability to find the existence of a central server, I assume it could not. However, whether or not the web browser used in the Kazaa installation is Microsoft Internet Explorer, it does not seem to be a browser that automatically blocks pop-ups. These are rife on the Kazaa webpages. That is not surprising. As Professor Tygar pointed out, the pop-ups are often advertising displays. Advertising revenue is the life-blood of the Kazaa system. It is inconceivable that Sharman would ever supply a web browser that blocked pop-up displays. Accordingly, while I have no reason to doubt the correctness of Professor Tygar's statements about some browsers being able to block pop-ups, those statements seem to have no relevance to this case. I am not prepared to say Mr Morle was wrong in disagreeing with Mr Hempel's view that the lack of an alternative would compel users to upgrade. However, I also see no reason to reject the 'drive them mad' concession that Mr Bannon extracted from Mr Morle. In a practical sense, I believe, Sharman could 'persuade' users to take the upgrade if they wished to continue to enjoy using Kazaa.

(h) Gold file flood filter

310 I have already mentioned the agreement between Sharman and Altnet concerning display of gold icons on KMD and Kazaa Plus. The display of gold icons is governed by TopSearch, software that is controlled by Altnet. Counsel for the applicants argued this control provides a ready means of denying users access to copyright material that is identified on a keyword list. They said:

> *'The Respondents could have created Gold Files which consisted simply of a copyright infringement warning,* 200 *copies of which appeared in response to a keyword search associated with the Applicants' sound recordings or their artists. ... The effect of* 200 *copies would be to flood the Kazaa user's search results page. Mr Morle regarded the flooding of the search results page with Gold Files as an effective means of inhibiting downloading of unauthorised Blue Files.*
>
> *No alterations to the software would be required to achieve that outcome. The Gold File list and associated keywords are able to be updated on a regular basis.*
>
> *The Respondents' request to include the Applicant record companies' catalogues of sound recordings as Gold Files demonstrates the Respondents' belief that their system can handle effective keyword links to the whole of that catalogue.'* (footnotes omitted)

It is desirable to refer to the evidence cited in support of these submissions.

311 Rodney McKemmish is a director of KPMG Forensic. He was called by counsel for the Altnet respondents to explain the Altnet technology, based on his observations and material he had read. The explanation was welcome, although it was never explained to me why counsel preferred that course to calling somebody, like Mr Rose, who had been involved in developing the technology and/or who worked with it on a daily basis.

312 During cross-examination by Mr J Nicholas SC for the applicants, Mr McKemmish agreed that KazaaLib provides for a limit of 200 results to be displayed in answer to an inquiry. Mr McKemmish agreed this meant that it would be possible to saturate the GUI display with gold files, leaving no room for

blue files that contained a name included on a keyword filter. He gave this evidence:

> *'It would be open to, at a technological level, Altnet, to create a sufficient number of gold files that were produced in response to a key word search for, for example, Delta Goodrem, to exclude from user's view, any blue files that might be otherwise retrieved using a search of that name? --- That's a possibility. Yes.*
>
> *And that would in effect involve, following up that specific example, registering, within the Altnet system, Delta Goodrem as a key word, wouldn't it? --- Yes, that's correct.*
>
> *And associating it with a collection of gold files? --- That's correct, yes.*

313 Mr McKemmish also gave this evidence:

> *'Can I ask you this, of course there is no reason why there needs to be any content in any of those files at all, is there? --- No, there doesn't have to be.*
>
> *They could be blank? --- That's correct.*
>
> *But they could be doing no more than occupying the user's screen and thereby denying the user access to blue files that might otherwise be retrieved? --- That's definitely a possibility.*
>
> *And Altnet can create those files, empty or otherwise, can't it? --- That's correct, yes.*
>
> *And of course they can also, as reflected in this proposal, prepare files that when clicked on generate warnings of one kind or another? --- That's correct, yes.*
>
> *So that in effect what the existing technology permits Altnet to do is to not only deprive a user of access to blue files but also to generate pop up warnings of one kind or another? --- Based on the material here, yes.'*

314 As appears at para 310 above, counsel for the applicants asserted that Mr Morle regarded the flooding of the search results page with gold files as an effective means of inhibiting the downloading of unauthorised blue files. I am not sure that is correct. However, at counsel's transcript page reference, Mr Morle did give this evidence:

> *'And in any event, as you say, the vision of Sharman is the promotion of the distribution of gold files. Do you agree with that? --- Yes.*
>
> *Anything which would stop the distribution or interfere with the distribution of blue files, doesn't interfere with the vision of distribution of gold files, does it? --- No.*
>
> *You agree with me? --- I agree that blue files don't affect gold files.*
>
> *Yes, and what I'm suggesting to you is anything which might inhibit the distribution of some blue files is not going to interfere with the vision of the distribution of gold files? --- Not that I can think. No.'*

315 That seems to mean it would be possible to adopt the course discussed by Mr Nicholas with Mr McKemmish without intruding on Altnet's entitlement to use the Kazaa system for the provision of licensed material and Sharman's asserted 'vision' to promote that use.

316 The reference by counsel for the applicants to a request to include the applicants' catalogue of sound recordings as gold files, is a reference to letters sent by Mr Bermeister to each of the six original applicants in this proceeding on 30 September 2004 in which he said:

> *'We would like to initiate discussions with you with a view to forming a business relationship between our respective organisations. Your organisation asserts copyright ownership and may wish to structure such a relationship upon a licence and we are open to any form of appropriate arrangement which protects the respective interests and claims of the parties and which will allow end-users of the KMD and other applications through which Altnet is distributed to download sound recordings to the mutual benefit of your organisation and ours. Importantly those benefits will lead to increased royalties which will flow through to those recording artists who provide the foundation for your organisation's commercial success. In conjunction with protection of all material the subject of any arrangement Altnet can provide related advertisements which would be prominently displayed in the KMD. This is a proven and effective business model for distribution and sale of sound recordings and films in the context of the Internet.*
>
> *Altnet will continue to market DRM protected games, music and movies for individuals and companies who want to enjoy the benefits of the P2P model. As indicated above a number of independent entities are currently working with us and establishing this market place. If your organisation wants to access the benefits that can be provided by well developed and recognised international digital distribution systems based upon the use of our software products, Altnet is poised and willing to provide such a vehicle. We have no preconceived notions concerning pricing of music or movies on a per play, per album, per day per month or other basis. All reasonable options are possible.*
>
> *We wish to work together with you as partners, to find a mechanism for commercial success. People clearly want to access sound recordings and films without having to leave their homes or the offices or web sites they are most satisfied with. The sheer volume of material available from a world-wide distribution partnership presents extremely exciting and affordable pricing options. We believe that a well organised plan to work together would give consumers what they are really seeking.*
>
> *Please let us know whether you are willing to consider our approach and, if so, when discussions can commence.'*

317 In para 216 above, I mentioned the Altnet Phase 2 document. Counsel for the applicants drew attention, in the present context, to a section of that document headed: 'Means of Tagging Altnet Files in Kazaa'. The author of the document was concerned about the possibility that a Kazaa user might download an Altnet file (a gold icon work) into his or her Kazaa Share folder and this might lead to the file being shared out to other users without recompense to Altnet. The perceived problem was not unlike the concern of the applicants that underlies this proceeding.

318 The Altnet Phase 2 document examined three possible ways of protecting Altnet's interests. Possibilities

1 and 3 were rejected on technical grounds. Possibility 2 was discussed as follows:

> *'**We supply Kazaa with periodic updates of all Altnet files in its Share folder***
> *Every few minutes the TopSearch DLL could scan the Kazaa Share folder for all files that it recognizes as Altnet files (it might recognize the files by comparing their size and file hash with the corresponding information contained in the TopSearch index). The TopSearch DLL would then call Kazaa periodically, giving it a list of all the files in the Share folder which are Altnet files. Kazaa would then not share out these files. This solution is fairly easy for Sharman to implement, but the danger is that Altnet may be pressured into modifying the TopSearch DLL to tell Kazaa that all files in the Kazaa Share folder are Altnet files, thereby preventing Kazaa from sharing any files and effectively shutting down the Kazaa network.'*

319 In their Closing Submissions, counsel for the applicants made this comment about that suggestion:

> *'In other words, TopSearch has the capability of identifying all files in the My Shared Folders of all Kazaa users and comparing that information with the filehash and other descriptions of Altnet files. It can then cause KazaaLib not to share out those particular files. This capability is something which is a continuous capability. Mr McKemmish's evidence that he could not see evidence of that capability in the software which he assumed was the TopSearch software does not answer the effect of this document for reasons previously given.'*

320 As counsel recognised, Mr McKemmish gave evidence relevant to this suggestion. He spoke of the ability of the TopSearch software to monitor searches for, and the downloading of, gold files. Apparently TopSearch already records 1% of all successful searches. Altnet treats this as a reliable sample from which to determine the demand for particular gold files. Mr McKemmish agreed it would be possible to extend recording to 100% of all searches, if required, without changing the user's software program.

321 It was unclear to me whether Mr McKemmish's discussion of these matters related only to gold icon results or to blue icons as well. He explained the position in this way:

> *'... you earlier said it would be possible for Altnet to collect statistical information about searches, and then this led on to a question about putting material that reacted to a particular search, to take the document's example of "Lolita". Now, what I want to clarify is, would that apply if a person was putting the word "Lolita" in ... with the intention of getting ... the offer of ... something on blue files, would it still be possible for Altnet - or for the system - to know that that was being put in and insert the warning, is that what you're saying? --- No, your Honour, there is a difference between the blue file and gold file. What happens is that the searching, if I put the key term "Lolita" in, in terms of the blue file, that search mechanism is performed through the FastTrack overlay network. In terms of gold files, that's passed to the TopSearch dll file, which is a local file, program file, and that search occurs locally on the computer and any matching gold files, and this is what this relates to, is looking into that data base, that local data base, would show you a gold file match. The blue file search would occur separately ...*
>
> *There are two different things really that Mr Nicholas has discussed with you. One is collection of statistics about what people are looking for? --- Yes.*
>
> *You were talking about that in the context of gold files only, were you? --- That's correct, your Honour.*

And ditto, the question of warnings such as a reaction to typing in the word "Lolita"? --- Yes. Yes, your Honour.

You didn't intend your answers to deal with people who are looking for shared files on the blue file system? --- That's correct, your Honour.'

322 The author of the Altnet Phase 2 document seems to have believed that TopSearch could monitor users' share folders in order to identify any Altnet files contained within them, apparently by comparing their size and file hash with corresponding information contained in the TopSearch index. Presumably, the reason why TopSearch cannot presently identify particular non-Altnet files held in users' share folders is that it does not have data concerning their size and hash numbers. If this information were to be supplied by interested copyright owners, it seems there would be no difficulty in detecting the presence of particular works in users' share files; at least unless and until the relevant hash number was corrupted or changed.

323 The author of the Altnet Phase 2 document commented that '[t]his solution is fairly easy for Sharman to implement'. The solution was rejected for the reason, curious to my mind, that Altnet might be 'pressured' (by whom?) into giving false information to 'Kazaa'; presumably Sharman. It is also interesting to note the author's belief about the effect of such conduct. As I understand the position, in the absence of any Altnet witness, Altnet only has music files. So the pressure would presumably extend only to music files. The author thought the result of preventing Kazaa to share music files would be effectively to shut down the Kazaa network.

324 Counsel for the applicants noted that the Altnet Phase 2 document went on to propose, as the 'fastest, most practical and most robust solution', modification of the KazaaLib as follows:

'□ When the user clicks to download a gold icon the Kazaa GUI tells the Kazaa LIB to set the "Don't Share" flag in the file's metadata stored in Kazaa's db file (this should be easy to do because the LIB file already allows users to right-click on a file and choose to not share it).
• In addition to setting the 'Don't Share" flag, the Kazaa GUI should also tell the LIB to set a "Gold Icon" flag for that file.
• The LIB file will now automatically not share out the file, even if the user moves it around or renames it (no extra work is required – the LIB file already does this – easy!)
• The LIB file can now also tell the Kazaa GUI that this is a Gold Icon file, and the GUI can then easily display the file with a gold icon, even in My Kazaa view.'

325 Counsel for the applicants commented, in their Closing Submissions, that this:

'involves requiring the Kazaa GUI to set a "Don't Share" flag in the metadata of a Gold File when a user downloads it. That ensures that that file cannot be shared out even if the Kazaa user moves it around or renames it. If TopSearch can do all of the above to control the movement of Gold Files it can readily do the same for other files. Copyright infringing files can be identified by their metadata and by their file hashes. TopSearch has the capacity to maintain and update a list of such files, search for such files in Kazaa Users computers and ensure that they are not shared. Again, the fact that 100% effectiveness may not be achievable is seized on by the Respondents' experts as being a reason for not doing it at all. It is not.'

326 It seems that Altnet has discussed with United States regulatory authorities the possibility of preventing, or inhibiting, people from using peer-to-peer technology for the exchange of pornographic material. Altnet has indicated it could insert a warning that would pop up each time a user searched for a word that was included on a list supplied by the Federal Bureau of Investigation.

327 Having regard to the Altnet Phase 2 document and the evidence of Mr McKemmish and Mr Morle on this point, there seems to be no reason why the respondents could not take the course suggested by counsel alternatively to, or cumulatively with, use of a filter system based on titles and performers' names.

328 The beauty of the gold file flood filter proposal, as I understand it, is that it does not depend on an existing user deciding to 'upgrade' to a new version of Kazaa. In effect, all items on the list of copyright works provided by copyright owners become gold file items. The metadata and file hash data of those items is transmitted by TopSearch to users' computers so that any search by a user for such an item will yield a 'gold file' response which consists, not of the work itself, but a 'don't infringe copyright' or 'don't share' notice. The implementation of such a system is a matter totally within the power of the respondents. As counsel for the applicants accept, it may not prove to be 100% effective, but it would significantly reduce Kazaa file-sharing copyright infringement. It seems also to have the advantage of avoiding 'false positives' that would trespass on other peoples' rights.

329 Any concern that it would be difficult for the Altnet system to provide blank file responses to the considerable number of works that would be likely to be listed by copyright owners cannot survive consideration of the letter from Mr Bermeister quoted at para 316 above. If Altnet can accommodate all the applicants' copyright works as licensed music files, without overburdening the capacity of its program, it surely can accommodate the same works as blank files.

330 The point was made by counsel for some of the respondents, and in relation to any filtering proposal, that the mechanism could not be made specific to Australian users; it would also constrain the access of non-Australian users to the copyright material included on the relevant copyright-owner's list. That is so, but I cannot regard that as an objection to a filtering mechanism. If it is reasonable for the respondents (or any of them) to adopt a filtering mechanism in order to avoid an infringement of Australian copyright law, it is immaterial whether that step would also have been necessary in order to avoid infringement of the copyright law of some other country.

(iii) Non-technological controls
(a) Warnings

331 Counsel for the applicants argued the current warnings on the Kazaa system are inadequate. They said:

> (i) there was no specific warning about infringement of copyright in sound recordings, despite Sharman's knowledge that the downloading of sound recordings was the predominant use of Kazaa and, because of that fact, users would tend to believe this practice was legal;
> (ii) this deficiency was exacerbated by the prominent statement on the website since the November 2004 launch of version 3, "Having Kazaa is 100% legal";
> (iii) the warnings do not explain that music files which appear in search results are likely to be subject to copyright and that, by making that file available online to the public through the use of My Shared Folder, and thereafter transmitting on request,

the user will be infringing copyright;
(iv) unlike advertisements and, to some extent, the websites, the warnings are not country specific. 'The generality of the warnings in relation to copyright infringement render them useless'. The warnings merely say that use of the software to download or share copyrighted works without the permission of the copyright owner '**may** be illegal in many jurisdictions'. (Counsel's emphasis);
(v) the respondents could have caused a gold file warning to appear in response to a search request for the applicant's sound recordings of artists, informing the user that by sharing or downloading this recording the user would breach copyright;
(vi) at the least, the respondents could have ensured that the Instant Messaging function was not capable of being disabled, thereby permitting the respondents to deliver warnings to all users.

332 The Sharman respondents adduced evidence about warnings from Geoffrey Bruce Stalley, a business consultant in the field of information technology. Mr Stalley said he had been asked to provide an opinion about the following matters:

> *'(a) what steps are ordinarily taken by a software vendor/licensor distributing its software product via the Internet to bring to the attention of a licensee of that software the terms and conditions on which the software is licensed?*
>
> *(b) having observed the installation process of the KaZaA Media Desktop on a computer owned by me, the extent to which the vendor/licensor of that software has brought to the attention of a licensee of that software the terms and conditions on which the software is licensed?*
>
> *(c) whether the matters referred to in (b) above are in my opinion, reasonable and consistent with industry practice?'*

333 Mr Stalley explained:

> *'In retail markets, software is generally sold by way of a contract between the vendor of the software and an end user. This contract invariably includes a licence of the copyright in that software to the end user and for that reason is generally referred to as an "end user licence agreement". This contract can be in hard copy or electronic form (where software is sold over the Internet). Hard copy contracts are often "shrink-wrapped" with software products in that the terms and conditions of the contract are enclosed with, or form part of, the packaging for the product and the purchaser in opening the product and installing the software is taken to have agreed with, and adopted, those terms and conditions'*

334 Mr Stalley said:

> *'It is generally the case that the terms of the end user licence agreement cover:*
>
> *(a) what the user is allowed to do with the software (usually focused on protecting the vendor's intellectual property in that software, ie. not allowed to make copies of, or alter the software);*

(b) warranties provided in relation to the usability of the software (usually limiting the vendor's responsibility for any damage to the user's data or systems by failure or problems associated with the vendor's software);

(c) rights of other parties (usually third party software or links included with the product);

(d) indemnifications (provided or not provided by the vendor); and

(e) limitation of liabilities (usually by the vendor).

It is becoming more common that the end user licence agreement also outlines a range of social and other possible legal issues that the end user should be made aware of before using the software (usually associated with the use of the software to transmit unauthorised or illegal information).

In a situation where a vendor is proving 'freeware' (ie. software at no cost to the end user) either as an upgrade to an existing product or as a product in itself, then the end user is generally expected to agree to terms similar to those outlined above.'

335 Mr Stalley annexed to his affidavit copies of the KMD v2.7 and Altnet EULAs. Mr Stalley summarised their contents and expressed the opinion they 'appear to reflect the generally accepted end user licence terms that are associated with the purchase of software over the Internet'. He thought the manner in which the terms were brought to the attention of the end user 'is reasonable and completely consistent with industry practice'.

336 Under cross-examination by Mr Bannon, it quickly became evident that Mr Stalley had never been required to advise clients in relation to peer-to-peer file sharing. His professional experience was limited to protection of the copyright interests of providers of licensed software. He had never used Kazaa and did not know much about it. He gave this evidence:

'Do you know enough about the operation of the Kazaa software that you can search for, by way of example, the name of a musical artist? --- I do know you can do that, yes.

Are you aware that the result of the application of that search will often produce search results, which will identify particular files. Are you aware of that? --- Yes, that is what I expect to happen. I haven't seen that but, yes, that is what I understand.

Well, are [you] aware that there is a download icon situated next to a particular successful search result files? --- I haven't seen the software to that level, but I'll assume that that is correct.

May we take it that you are now aware that, in the case of a musical file, which was identified in the search result, in response to a search, that there is no indication in the search folder as to whether or not clicking on that download button by the Kazaa user would or would not infringe any copyright. Are you aware of that? --- No, I'm not but I don't know the answer to that.

Would you have any idea - well, how would you expect the user of the system to know whether

or not clicking on that download button would or would not infringe any copyright? --- I don't know the answer to that.

Do you have any idea of what provisions of the copyright potentially clicking on that download button might be infringed? --- No.

Have you ever heard of the exclusive right of an owner of copyright and of sound recording to communicate the sound recording? --- Are we saying a record, or a CD, or the music is theirs?

Have you ever heard of the exclusive right of an owner of copyright and of sound recording to communicate that sound recording to the public? --- I don't know what that means.'

337 I have considerable doubt that this is an area in relation to which expert opinion is admissible. It certainly appears to be unnecessary. A judgment about the adequacy of a warning is a conclusion of fact, having regard to the circumstances of the case. What appears to be an emerging practice of calling experts to guide judges in relation to simple jury questions is to be deprecated. However, even if it was legitimate for Sharman to call a witness to deal with the matter, Mr Stalley was not a good choice. I do not think he has anything to contribute to determination of the sufficiency of the Kazaa warnings.

338 Counsel for the Sharman respondents put a number of arguments concerning the adequacy of Sharman's warnings. They emphasised that the warning about copyright infringement appeared on each page of the website, reference being made to the terms of the EULA. Counsel said the:

'statements and warnings are made or given in circumstances where it is notorious that the swapping between users of copies of commercial sound recordings by way of the Internet is not authorised by the owners of the copyright in such sound recordings and notorious that the use of the KMD to swap copies is not authorised by the record companies that own the copyright in those recordings.'

339 Counsel argued the website statement that 'having' Kazaa is legal indicates that, while having the software is legal, using it to infringe copyright is not. Counsel said the warnings are in the English language and in clear terms. The EULA makes it clear that the user is responsible for ensuring that he or she is authorised to download or share copyright works. Because these statements were clear, counsel submitted:

'... there was no need for the Sharman Respondents to cause a gold file warning to appear in response to any search request or send some form of instant message in circumstances where there was a clear warning as to copyright infringement, and those to whom it was given could reasonably be taken to be aware that swapping copies of commercial sound recordings via the KMD was not authorised by the Sharman Respondents or the record companies who owned copyright in those recordings.'

340 Counsel for the Sharman respondents based their claim about the notoriety of the fact that file-sharing of commercial sound recordings infringes copyright entirely upon the circumstance that the applicants so asserted in para 80 of the S of C. This is a dubious basis. There is no evidence about the matter. I have no reason to believe any significant number of Kazaa users, apparently mainly teenagers and young adults, has any knowledge about, or interest in, copyright law or its application to file-sharing. Nor have I any reason to believe that any significant proportion of users would care whether or not they were infringing copyright. The 'Join the Revolution' material displayed on the Kazaa website and the 'Kazaa Revolution' T-shirt

indicates the Sharman respondents perceive they might not. While I agree with the applicants that the existing warnings do not adequately convey to users what constitutes breach of copyright, I am not persuaded it would make much difference if they did.

(b) Enforcement by legal action

341 Counsel for the applicants criticised the fact that, although they knew many users habitually infringed copyright, the respondents have never taken action to enforce the relevant terms of the licence agreement. They said:

> *'Leaving to one side the disputes in the evidence relating to the Respondents' ability to monitor generally, there is and was an undoubted capacity to monitor individual user's activity by undertaking searches on the system of the very type undertaken by persons on behalf of the Applicants for the purposes of evidence in these proceedings.*
>
> *The Respondents could have undertaken such searches and could have identified the existence of files being made available in a user's My Shared Folder which appeared to be infringing the Applicants' copyright. The IP address of that user could have been identified and ascertained as an Australian user. On the assumption that information that the file in the My Shared Folder accurately reflected its description in the search result, Sharman had a clear right to commence legal proceedings for an injunction to restrain the continued use of the software by the user in breach of the licence conditions. The existence of those circumstances would have entitled Sharman to download the file to check the accuracy of the description for the purposes of evidence in those proceedings. The IP address of the relevant user could have been recorded along with the time and date of the recording. The evidence is that with that information, and with the assistance of the relevant ISP [Internet Service Provider] provider, the identity of users can be ascertained regardless of the potential for IP addresses to change.*

Counsel said preliminary discovery proceedings against the relevant ISP would have enabled Sharman to gain the necessary information upon which to base a case.

342 Evidence was given by Michael Charles Bates, a registered patent and trade mark attorney called by the applicants, that changes to the registry of a user's computer, on the installation of Kazaa software, included insertion into the computer's random access memory of instructions 'to probe the user machine for the local IP address (whether public or private), the traffic in and out of the computer, the number of downloads and uploads, and the Supernode list as well as other activity'.

343 Professor Tygar gave evidence that many computers have changing IP addresses. To address this problem, he said, two techniques are used together. First, web servers are normally assigned static IP addresses, that is IP addresses that do not change or change infrequently. Second, there is a complex system of special name servers ('the Distributed Name Service' or 'DNS') 'that allows an alphanumeric name, such as the web server www.fedcourt.gov.au to be translated into an IP address such as 152.91.44.238'. He described technical problems associated with DNS.

344 Professor Tygar also said:

> *'IP addresses are assigned in groups to Internet Service Providers (ISP) who in turn make the IP addresses available to their subscribers. Since ISPs divide along national boundaries, IP*

addresses normally should indicate the Internet Service Provider being used and thus the country of origin of messages. However, here there are difficulties. It is common to redirect messages through an intermediate machine called a proxy*. Messages appear to be coming from that proxy and thus the proxy anonymizes the IP address. (Some proxy services even advertise that they will anonymize requests.) Because of mechanisms such as proxies, it is not even possible to accurately identify the country in which a computer is being used. For example, UC Berkeley maintains an electronic library which has a number of resources only available to faculty and students at Berkeley. When I am on the road, I can use a proxy provided by the University to access these resources – my requests appear to be coming from the UC Berkeley campus, even if I am far away. These proxy services are not at all esoteric or rare; in fact, popular web browsers including Microsoft's Internet Explorer include extensive support for proxies easily available to the user.'*

345 Professor Ross also gave evidence on this subject, more detailed but to the same general effect.

346 Nigel John Carson, Director Computer Forensics at Ferrier Hodgson, responded to Professor Tygar and Professor Ross in this way:

'Information about IP addresses that are dynamically assigned (or even obfuscated by Network address translation) is used on a regular basis and very successfully by the police, regulatory authorities and other investigative bodies to identify the physical location and exact computer from which the communication being investigated using that IP address originates. They are able to do this based on the following other information that is usually also available in addition to the IP address if any investigation is undertaken:

(a) the time and date of the communication (regionally specific if necessary);
(b) The internet port number/s and transport types (UDP/TCP) that the IP address was communicating on;
(c) the "who is" records of the entity to whom that IP address or range of IP addresses has been allocated;
(d) trace routes to the IP address and looking glass trace routes to identify approximate geographic location;
(e) the DHCP connection logs of the allocating authority for that IP address (usually an ISP) combined with the time/date information will generally provide a user account associated with the IP address at the time in question;
(f) the account information can then be used to identify a physical address from which the computer that used that IP address is operating; and
(h) once the above information has led to the originating local network from which the communication was issued, the gateway on that network will often contain logs mapping IP address information to Media Access Control (MAC) addresses which will uniquely identify the network interface card from which the communication was issued. This ties the communication to the physical originating computer.

In some instances, there can still be potential difficulties in this process that are faced day to day by police and regulation authorities to identify individuals and users on the Internet. One issue is that the physical address may be a business that contains hundreds of computers whose IP address has been hidden through the use of a Network address translation router. However,

even in these cases, the relevant router often maintains logs that map internal IP addresses to internet ports at particular times or the computer in question can be tracked down by a local network scan looking for a particular open service (such as port 1214 for supernode communications). So in this sense the IP address and time is the starting point for the identification of the communicating computer.

I have used the above-described investigative process in more than twenty computer forensic operations both within the police service, for the government and in the corporate sector to successfully locate computers that are using dynamically assigned IP addresses, including in these proceedings. I cannot recall any instance where using an investigative process that involves using IP addresses, even dynamically assigned IP addresses, has failed to identify a target computer.'

347 In oral evidence, Mr Carson said he used this method to find the computers at Queensland and Monash Universities that were being used as Kazaa supernodes.

348 Under cross-examination by Mr Meagher, Mr Carson said it is necessary to have some compulsive power in order to obtain information from Internet service providers: 'they are not going to give these records to just anybody'. However, he was not challenged by Mr Meagher (or anyone else) about his assertion that he had always been able to identify target computers, using IP addresses.

349 In their Closing Submissions, counsel for the Sharman respondents made several comments about this suggestion. They pointed out the applicants, themselves, had not chosen to commence proceedings against infringing users. They emphasised, as Mr Carson conceded, that some form of compulsory process would be necessary. In relation to the possibility of preliminary discovery, they asked why their clients should be 'expected to embark on expensive and uncertain litigation in circumstances where the copyright owners are in a better position to commence and prosecute a proceeding'.

350 Counsel also mentioned difficulties in obtaining information about use. Counsel pointed out that MediaSentry's investigation involves the use of a large bank of computers, containing highly specialised software, whose development involved about 6,000 hours work, access to which MediaSentry would not allow Sharman.

351 There is force in these points. Perhaps the occasional legal proceeding might be useful '*pour encourager les autres*', if the necessary information could be obtained. However, it is not realistic to believe legal action against individual infringers will stamp out, or even significantly reduce, file-sharing infringements of copyright.

V THE AUTHORISATION ISSUE

(i) The statutory provisions

352 This case requires consideration of a number of provisions of the Act, including some amendments made by the *Copyright Amendment (Digital Agenda) Act 2000* ('the 2000 Act') that have not previously been judicially considered.

353 Part IV of the Act relates to copyright in subject matter other than works. As defined in s 10 of the Act, 'work' means a 'literary, dramatic, musical or artistic work'. Part 1V contains ss 84 to 113C.

354 By virtue of s 85(1) of the Act, unless a contrary intention appears, the owner of the copyright in a sound recording has the exclusive right to do all or any of the following acts:

> *'(a) to make a copy of the sound recording;*
>
> *(b) to cause the recording to be heard in public;*
> *(c) to communicate the recording to the public;*
>
> *(d) to enter into a commercial rental arrangement in respect of the recording.'*

355 Section 10 defines the term 'sound recording', for the purposes of the Act and subject to any apparent contrary intention, as 'the aggregate of the sounds embodied in a record'. The word 'record' means 'a disc, tape, paper or other device in which sounds are embodied'. The respondents accept the Defined Recordings all fall within the definition of 'sound recording'.

356 It will be noted that s 85(1)(c) refers to the right 'to communicate the recording to the public'. Two definitions, added by the 2000 Act, are relevant to that paragraph. They apply subject to any indication of a contrary intention. First, 'communicate' relevantly means:

> *'make available online or electronically transmit (whether over a path, or a combination of paths, provided by a material substance or otherwise) a work or other subject-matter.'*

Second, 'to the public' means 'to the public within or outside Australia'. Accordingly, a copyright owner has the exclusive right, amongst other things, to make available online, or electronically transmit, a work to members of the public, whether they be inside or outside Australia.

357 Section 101 deals with what has been called 'primary infringement'. Subsection (1) of s 101 says that, subject to the Act, a copyright subsisting by virtue of Part IV:

> *'is infringed by a person who, not being the owner of the copyright, and without the licence of the owner of the copyright, does in Australia, or authorizes the doing in Australia of, any act comprised in the copyright.'*

358 The authorisation referred to in s 101(1) extends only to direct authorisation, by a potential defendant, of the person who performs the infringing acts. However, the applicants argued that s 13(2) of the Act takes authorisation one step further. That subsection provides:

> *'For the purposes of this Act, the exclusive right to do an act in relation to a work, an adaptation of a work or any other subject-matter includes the exclusive right to authorize a person to do that act in relation to that work, adaptation or other subject-matter.'*

359 The 2000 Act inserted into s 101 a new subsection (1A), dealing with determination of the question whether a person has authorised the doing in Australia of an act, comprised in a copyright subsisting by virtue of Part IV of the Act, without the licence of the copyright owner. The matters to be taken into account include:

> *'(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.'

360 Counsel for the applicants made a number of points concerning s 101(1A). They may be summarised as follows:

(i) The words 'if any' in s 101(1A)(a) indicate the possibility 'that a person with no power to prevent the doing [of] the act concerned may nevertheless, by the interplay of the other factors prescribed, authorise infringement'. Counsel say this 'plainly supersedes' the first proposition stated by Gibbs J in *University of New South Wales v Moorhouse* (1975) 133 CLR 1 ('*Moorhouse*').
(ii) The words '**other** reasonable steps to prevent or **avoid'** (counsel's emphasis), in s 101(1A)(c), show it is material to consider the availability, and taking, of steps falling short of prevention.
(iii) The composite phrase 'prevent or avoid' is reminiscent of 'prevent or inhibit', used in the definition of 'technological protection means' in s 10 of the Act. That phrase has been held to cover acts of deterrence and discouragement: see *Kabushiki Kaisha Sony Computer Entertainment v Stevens* (2003) 132 FCR 31 at 39 (French J) and 55 (Lindgren J).
(iv) Section 101, as amended in 2000, must be read in conjunction with s 112E, also introduced by the 2000 Act. Section 112E operates as an exception to s 101. It states:
'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.'

By virtue of s 100A of the Act, the term 'audio-visual item' in s 112E includes a sound recording.

361 The significance of s 112E, according to counsel for the applicants, is that 'the new ambit of authorisation in s 101 means that (but for s 112E) a person who provides facilities for the making of a communication would be taken to authorise an infringement of copyright **merely because** another person **uses the facilities** so provided to do something which is included in the copyright'. (Counsel's emphasis)

362 Reference should also be made to s 22(6) of the Act, which was cited by counsel for the Altnet respondents. That subsection reads:

'(6) For the purposes of this Act, a communication other than a broadcast is taken to have been made by the person responsible for determining the content of the communication.'

The term 'broadcast' is defined, by s 10 of the Act, as 'a communication to the public delivered by a broadcasting service within the meaning of the *Broadcasting Services Act 1992*'. A communication effected by Internet file sharing is clearly not within this definition; consequently, s 22(6) applies. However, the subsection relevantly does no more than to establish that a user who determines the content of the material

that he or she will download from another user's computer is to be taken as having made that communication. Whether or not the communication has been authorised by someone else is another matter. Section 22(6) says nothing about authorisation.

(ii) Submissions of counsel

363 Counsel for the applicants argued that, as by s 101(1) an act of authorisation is itself an infringing act, s 13(2) has the effect of making it an infringing act for a person to authorise someone else to authorise any of the actions listed in s 85(1). They said this understanding of the position is consistent with a statement of Gummow J in *WEA International Inc v Hanimex Corporation Ltd* (1987) 17 FCR 274 (*'Hanimex'*) at 281:

> *'Copyright in relation to a sound recording is the exclusive right, inter alia, to make a record embodying the recording and that exclusive right includes the exclusive right to authorise a person to make a record embodying the recording ... It should however be noted that the concept of authorisation appears both directly and indirectly in the statutory description of infringement. That is to say, it appears in terms in the infringement section, s 101(1) and it also appears indirectly therein because the expression in s 101(1) "any act comprised in the copyright" itself imports the concept of authorisation through the operation of ss 13 and 85.'*

364 At 283, Gummow J commenced a discussion of the concept of authorisation and of its case-law history. He did so on the basis, expressed at 284, that the 'concept of "authorisation" in the legislation had its own independent operation from what one might call primary infringement'. The approach was endorsed by a Full Court (Sheppard, Foster and Hill JJ) in *Australasian Performing Right Association Ltd v Jain* (1990) 26 FCR 53 (*'Jain'*) at 57.

365 It is convenient to say immediately that I have not found it necessary to reach a conclusion about the applicants' concept of authorising an authorisation. If that concept has validity, it seems to have no relevance to the facts of this case. The only question, in relation to the authorisation issue, is whether any of the respondents authorised Kazaa users to do either of the acts described in paras (a) and (c) of s 85(1) of the Act.

366 The term 'authorise' is not defined in the Act. However, in *Moorhouse* at 12, Gibbs J noted that, in legislation of similar intendment to s 36 of the Act (which is the provision of Part III corresponding with s 101), the word authorise 'has been held to have its dictionary meaning of "sanction, approve, countenance"'. Jacobs J (with whom McTiernan J agreed) also adopted this meaning.

367 Gibbs J went on to make some observations about what would constitute an authorisation. He thought the High Court's decision in *Adelaide Corporation v Australasian Performing Right Association Limited* (1928) 40 CLR 481 provided authority for three propositions:

> (i) 'A person cannot be said to authorize an infringement of copyright unless he has some power to prevent it';
> (ii) 'Express or formal permission or sanction, or active conduct indicating approval, is not essential to constitute an authorization. "Inactivity or indifference, exhibited by acts of commission or omission, may reach a degree from which an authorization or permission may be inferred"'; and
> (iii) 'However, the word "authorize" connotes a mental element and it could not be inferred that a person had, by mere inactivity, authorized something to be done if he neither knew nor had reason to suspect that the act might be done'.

368 In *Moorhouse* at 21, Jacobs J said:

> *'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 ...'* (reference omitted)

369 Jacobs J also said (at 21) that:

> *'[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'.*

370 Knowledge, or lack of knowledge, is an important factor in determining whether a person has authorised an infringement. However, it is not a conclusive factor. Just as there may be authorisation without knowledge, mere knowledge is not enough. In *Nationwide News Pty Ltd v Copyright Agency Limited* (1996) 65 FCR 399 at 422, Sackville J (with whom Jenkinson and Burchett JJ agreed) said:

> *'Nonetheless, a person does not authorise an infringement merely because he or she knows that another person might infringe the copyright and takes no step to prevent the infringement.'*

371 Counsel for the Sharman respondents argued that s 101(1A) did not change the law concerning authorisation. They said it was already clear that control is not necessary for there to be a finding of authorisation. They cited the decision of Herring CJ in *Winstone v Wurlitzer Automatic Phonograph Company of Australia Pty Ltd* [1946] VLR 338 at 347. Counsel also referred to the Revised Explanatory Memorandum for the 2000 Bill, which dealt with the proposed s 101(1A). After listing the matters that the new subsection required to be taken into account, that document stated at para 151:

> *'The inclusion of these factors in the Act essentially codifies the principles in relation to authorisation that currently exist at common law ... It is intended to provide a degree of legislative certainty about the steps that should be taken in order to avoid liability for authorising infringements. Additional certainty in relation to third party liability is provided by new s 101(1A)(c). This section specifies that compliance with relevant industry codes of practice is a factor in determining whether the person took reasonable steps to prevent or avoid the doing of the act.'*

372 Counsel for the Sharman respondents argued that s 101(1A) 'now prescribes certain matters that must be considered in determining the question of authorisation but it is an inclusive, not exhaustive, list'.

373 Basing themselves on the view that pre-2000 principles still apply, counsel for the Sharman respondents referred to some English authorities. In *Falcon v Famous Players Film Company* [1926] 2 KB 474 at 499, Atkin LJ said:

> *'[T]o "authorise" means to grant or purport to grant to a third person the right to do the act complained of, whether the intention is that the grantee shall do the act on his own account, or*

only on account of the grantor.'

374 In *CBS Songs Ltd v Amstrad Consumer Electronics PLC* [1988] 1 AC 1013 (*'Amstrad'*), the House of Lords considered a claim by the owners of copyright material against a manufacturer of high fidelity sound recording equipment with facilities for recording at high speed from pre-recorded cassettes on to blank tapes. The House of Lords unanimously upheld an order by the Court of Appeal striking out the plaintiff's claim. In doing so, the House considered the terms of the *Copyright Act 1956* (UK) and, in particular, s 1(2) of that Act. That subsection provides that copyright in a work is infringed by a person, not being the owner or licensee of the copyright, who 'authorises any person' to do any of the acts included in the concept of copyright embedded in s 1(1) of that Act.

375 Lord Templeman (with whom the other four members of the House agreed) stated (at 1054.C) that 'Amstrad did not sanction, approve or countenance an infringing use of their model'. He held that, in the context of the United Kingdom Act, 'an authorisation means a grant or purported grant, which may be express or implied, of the right to do the act complained of'. He said: 'Amstrad conferred on the purchaser the power to copy but did not grant or purport to grant the right to copy'.

376 Lord Templeman went on to note Gibbs J's reference to control in *Moorhouse*. He commented: 'Whatever may be said about this proposition, Amstrad have no control over the use of their models once they are sold.'

377 Lord Templeman also considered the plaintiffs' common law rights. At 1058 he said:

> *'My Lords, I accept that a defendant who procures a breach of copyright is liable jointly and severally with the infringer for the damages suffered by the plaintiff as a result of the infringement. The defendant is a joint infringer; he intends and procures and shares a common design that infringement shall take place. A defendant may procure an infringement by inducement, incitement or persuasion. But in the present case Amstrad do not procure infringement by offering for sale a machine which may be used for lawful or unlawful copying and they do not procure infringement by advertising the attractions of their machine to any purchaser who may decide to copy unlawfully. Amstrad are not concerned to procure and cannot procure unlawful copying. The purchaser will not make unlawful copies because he has been induced or incited or persuaded to do so by Amstrad. The purchaser will make unlawful copies for his own use because he chooses to do so. Amstrad's advertisements may persuade the purchaser to buy an Amstrad machine but will not influence the purchaser's later decision to infringe copyright. Buckley L J observed in* Belegging-en Exploitatiemaatschappij Lavender B V v Witten Industrial Diamonds Ltd *[1979] FSR at 65, that "Facilitating the doing of an act is obviously different from procuring the doing of the act." Sales and advertisements to the public generally of a machine which may be used for lawful or unlawful purposes, including infringement of copyright, cannot be said to "procure" all breaches of copyright thereafter by members of the public who use the machine. Generally speaking, inducement, incitement or persuasion to infringe must be by a defendant to an individual infringer and must identifiably procure a particular infringement in order to make the defendant liable as a joint infringer.'*

378 Counsel for the Sharman respondents accepted that '[t]he sale or distribution of something, the use of which will **necessarily** involve the doing of an act in breach of copyright, is likely to constitute an authorisation of the relevant use' (counsel's emphasis). They said 'the sale or distribution of something which is only capable of unlawful use is taken necessarily to authorise or sanction that use'. They argued

that *Moorhouse* was not a sale or distribution case; the photocopying machine remained under the university's control.

379 Counsel for the Sharman respondents also referred to *Australian Tape Manufacturers Association Ltd v Commonwealth of Australia* (1993) 176 CLR 480 ('*Australian Tape*'). The issue in that case was the constitutional validity of legislation imposing a 'royalty' upon blank tapes, the royalty being payable to a collecting society acting on behalf of copyright owners. By majority (Mason CJ, Brennan, Deane and Gaudron JJ; Dawson, Toohey and McHugh JJ dissenting), the High Court held the legislation to be invalid. At 497, in the course of discussing the question whether the levy was a royalty, the majority Justices said the 'sale of a blank tape does not constitute an authorization by the vendor to infringe copyright'. They said that was 'principally because the vendor has no control over the ultimate use of the blank tape'. Their Honours referred to *Amstrad* and to a similar decision (in respect of home video tapes) of the Supreme Court of the United States, *Sony Corporation of America v Universal City Studios Inc* (1984) 464 US 417 (*'Sony'*). [In the recent *Grokster* case, the Supreme Court affirmed the continuing correctness of *Sony*.]

380 In *Australian Tape*, at 498, the majority went on:

> *'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)

381 Several counsel in this case referred to the decision of Bennett J, in this Court, in *Australasian Performing Right Association Ltd v Metro on George Pty Ltd* (2004) 61 IPR 575 ('*Metro'*). In that case the first respondent hired out a venue for live performances, arranged by other people, of musical works, including works for which APRA held copyright. At various times, the second and third respondents were directors of the first respondent. The respondents did not authorise or permit any particular performance. Those hiring the premises were required to warrant they would ensure all performances complied with copyright obligations.

382 Bennett J saw the first question as being whether, for the purposes of s 36(1) of the Act, 'the respondents have authorised, in the sense of "sanction, approve or countenance" the infringement of copyright' by the presenters of live performances: see [16]. Her Honour referred to the authorities mentioned above, emphasising what was said about control in *Moorhouse, Amstrad* and *Australian Tape*. In the course of the reference, her Honour said at [19]:

> *'Express or formal permission or sanction or active conduct indicating approval are not essential to a finding of authorisation: .... While mere inactivity or indifference is insufficient, if there is no knowledge or reason to suspect that the particular infringing act might be done, inactivity or indifference, exhibited by conduct, by acts of commission or omission, may reach a*

degree from which authorisation or permission may be inferred: ... Declining to interfere may constitute acquiescence, particularly if the party was notified that the infringing work was probably going to be performed: ... However, mere indifference cannot be treated as "permission" unless there was some power to permit the performance and unless there was some duty to interfere:' (references omitted)

383 At [20], Bennett J noted that, in *Moorhouse*, Jacobs J thought an important question 'is whether there was an invitation to be implied that the users might make such use of the facilities as they thought fit'. Bennett J added:

'The likelihood of the occurrence of the infringing act is relevant, as is evidence of the degree of indifference displayed.'

384 At [22], Bennett J mentioned an earlier APRA case. She said:

'In Australasian Performing Right Association Ltd v Canterbury-Bankstown League Club Ltd *[1964–5] NSWR 138 (*Canterbury-Bankstown*), the club engaged an orchestra to play music for dances held at the premises. The band leader would select the music without reference to the club. The club had no knowledge of what music was to be played. It did not select it, was not asked for approval and was not consulted. However, the club provided entertainment of which music was an integral part. The person engaged to play music was given a general authority to play whatever music he liked irrespective of copyright. APRA had reminded the club that it controlled the rights of public performances in Australia of practically all current musical works and that the authorisation of a public performance of such music without a valid licence from APRA constituted infringement of copyright. Ferguson J, with whom Herron CJ agreed, held that, in giving to the band leader a general authority to play whatever music he liked irrespective of copyright, the club either performed or authorised the performance: at 140. Asprey J came to the same conclusion.'*

385 Bennett J did not attempt any general exposition of the significance of adding subs (1A) to s 36 of the Act. In response to a submission by the respondents about the effect of their requiring hirers to warrant compliance with copyright requirements, her Honour observed, at [44]:

'The inclusion of the warranty in the Metro contract was a reasonable step to take which, if implemented by the hirer, would have prevented an unlicensed performance. However, s 36(1A)(c) does not address steps to prevent or avoid infringement generally, rather it addresses steps to prevent or avoid the doing of the act itself, that is the act comprised in the copyright in a work. Metro did not take steps to prevent or avoid the performances.'

386 Bennett J ultimately held the corporate respondent, and one of the individual respondents, each to be liable for infringement of copyright on the basis of control. At [73], her Honour said:

'Metro was in control of the premises. Metro advertised the performances. It operated the box office, provided refreshments and provided and operated the electricity necessary for the performances to take place. The Metro contract formed the basis of the hiring of the premises. This may not have amounted to control over the content of the performances but, in my view, it gave a measure of control over the use of the premises in circumstances where Metro knew or had grounds to believe that unlicensed performances were to take place or were in fact taking

place at Metro on George.'

387 In a case decided after completion of argument in this matter; *Universal Music Australia Pty Ltd v Cooper* [2005] FCA 972, (*'Cooper'*), Tamberlin J made a comment about the factors listed in s 101(1A) of the Act. His Honour said at [81]:

> *'These factors are not exhaustive and do not prevent the Court from taking into account other factors, such as the respondent's knowledge of the nature of the copyright infringement.'*

388 Finally, it will be recalled that s 101(1) makes an infringement of copyright only the 'doing in Australia' of an act specified in s 85(1) of the Act. In the present case, it is apparent that many Kazaa users reside outside Australia; the infringing activity of these users is not done in Australia. However, it seems to me that this is immaterial. The evidence, both from Mr Mizzone and the focus group reports, is that copyright infringement also takes place in Australia. If the respondents, or any of them, authorise Kazaa users generally to infringe copyright, they authorise the doing of the infringing acts both within Australia and outside Australia. It does not matter that the latter activity is outside the scope of s 101 of the Act.

389 Counsel for Mr Morle supported the contention that s 101(1A) did not change the pre-existing law. Counsel said *Moorhouse* 'identified the meaning of "authorised" as "sanction, countenance or approve".' Counsel said:

> *'Distilled to its essence authorisation requires conduct which objectively can only be regarded as a grant or purported grant [of] approval or permission, given by the authoriser to the primary infringer to do the act of primary infringement. To be an authorisation the purported grant of approval or permission must be a cause of the act of primary infringement which is necessary for the authorisation itself to be complete. A mere exhortation cannot amount to authorisation.'*

Counsel went on:

> *'Section 101(1A) recognises this. A purported grant of permission will usually have that character, and thus be a cause of infringement, because the authoriser has the legal power, vis a vis the infringer, to grant or withhold permission or otherwise is in a particular relationship with the primary infringer which enables him or her to effectively control the latter's infringing conduct. That effective control provides the causal link with the primary infringement. Section 101(1A)(c) is directed to injecting some certainty into situations where there is no such power or relationship (*"third party" *situations in the language of the explanatory memorandum). It does not do away with the requirement that an alleged infringer must be shown, effectively, to have control over the act of infringement of the primary infringer for there to be authorisation.'*

390 Counsel for the Altnet respondents put s 112E of the Act at the forefront of their submissions. They said that section provides a complete defence to Sharman, and therefore all other respondents. Counsel said:

> *'The section is, expressly, not confined to carriers and carriage service providers, and the legislative history confirms that it was not intended to be so limited. (The* Copyright Amendment (Digital Agenda) Bill *1999 as first introduced was confined to carriers and carriage service providers, however the words of limitation were removed in a revised Bill*

introduced in 2000, and the revised explanatory memorandum in terms stated that the provision extended to "digital storage service providers" and "any other persons who provide facilities for making, or facilitating the making of, a communication"'.

391 In their Closing Submissions, counsel for the applicants put three arguments concerning the application of s 112E to this case:

'Firstly, on the assumption that the Respondents provide "facilities" for making communications, they do not "merely" provide such facilities. The matters relied on above clearly indicate that the Respondents have a commercial interest in the copyright infringing activities of the Kazaa users and seek to trade off that activity. [They] have taken steps which encourage and make that activity easier and more difficult to police as outlined above.

Secondly, the expression "facilities" ought to be understood as referring to physical facilities. The Respondents provide the software for making communications but no hardware in the form of computers, Internet cables or otherwise. The background materials to the introduction of the section suggest that it was introduced in the context of the introduction of the communication right in order to protect the providers of Internet facilities such [as] ISPs (Internet service providers). ISPs provide computers, routers and cabling which physically receive, store and direct communications.

If it be determined that by the provision of software the Respondents provide facilities for making communications, the implication of s 112E is that without its operation, the provider of those facilities would be authorising the making of such communications. On this basis, because the Respondents do more than "merely" provide such facilities, they bear the burden of s 112E without enjoying its benefit.

Thirdly, the Respondents themselves deny that they operated facilities in the manner in which a carriage service provider does.' (footnotes omitted)

392 The last paragraph referred to a letter dated 14 February 2002, from Sharman's then solicitors to solicitors acting on behalf of some of the applicants, in which the statement was made:

'Sharman is not a carriage or internet service provider. It does not host any activities on its web site other than the supply of the Software. It does not infringe the copyright of any third party nor does it authorise the infringement of third parties.'

393 Counsel for Mr Rose responded to these arguments by contending that:

> (i) the applicants' argument involves a 'relocation of the adverb "merely" from a position where it qualifies "is not taken to have authorised" to a position where it qualifies "provides"';
> (ii) there is no justification for limiting the word 'facility', to physical facilities.

Counsel said:

'The original exposure draft of the Copyright Amendment (Digital Agenda) Bill *1999, which was prepared in February 1999, contained a draft section 112C (ultimately section 112E)*

which provided [emphasis added]:

A carrier or a carriage service provider is not taken to have authorised any infringement of a copyright in a cinematograph film, a sound recording, a television broadcast or a sound broadcast merely because he or she provides ***physical*** *facilities used by a person to do something the right to do which is included in the copyright.*

In subsequent versions of the Bill the word "physical" was omitted, as it was from the precursor to section 39B. The Explanatory Memorandum for a later version of the Copyright Amendment (Digital Agenda) Bill *1999 included the statement:*

The reference to "facilities" is intended to include physical facilities and the use of cellular satellite and other technologies.

The legislative history of this provision (and its counterpart section, 39B) makes it quite clear that a conscious choice was made to omit the word "physical" and not limit the operation of the section in the manner suggested by the Applicants.'

394 The historical statements made in the quoted paragraph are correct. Counsel for Mr Rose are correct in arguing the word 'facilities' should not be confined to physical facilities.

(iii) The application of s 112E

395 The qualifying elements of s 112E apply to Sharman.

(i) Sharman is '[a] person' (it does not matter whether or not it is a carriage service provider);
(ii) Sharman provides facilities (it does not matter they are not physical facilities);
(iii) the facilities are 'for making, or facilitating the making of, a communication' (an Internet file-sharing transaction).

396 It follows that Sharman is a person to whom s 112E may apply. Therefore, the effect of s 112E is that Sharman is 'not taken to have authorised any infringement of copyright in a [sound recording] merely because [a Kazaa user] uses the facilities' to infringe the copyright. If the most that can be said against Sharman is that it has provided the facilities used by another person to infringe copyright, Sharman is not to be taken to have authorised the infringement. So understood, s 112E operates as a legislative reversal of the High Court's decision in *Telstra Corporation Limited v Australasian Performing Right Association Limited* (1997) 191 CLR 140 (*'Telstra'*).

397 There is good reason to believe such a reversal was the purpose of enacting s 112E. In July 1997, two Commonwealth Ministers, the then Attorney-General and the then Minister for Communications and the Arts, published a Discussion Paper entitled 'Copyright Reform and the Digital Agenda'. That paper made reference to the then recent decision of the Full Federal Court in *Telstra*. Paragraphs 4.87 and 4.88 of the Discussion Paper read:

'On the basis of the scheme proposed in this paper, it is intended that Telstra would as a carrier not be liable to APRA for the playing by others of music on-hold to users of mobile telephones, contrary to the result under the current law (in the Full Federal Court decision in

APRA v Telstra*).*

No proposals are made in relation to providing carriers or carriage service providers with a statutory exception from liability for infringement of the new rights proposed in this paper on the basis that the case law on the authorisation of copyright infringement is better able to adapt to developments in this area. We do, however, invite comment on whether the Copyright Act should be amended to provide that ISPs would be exempt from copyright liability in any circumstances in which they provided notices to their subscribers about copyright rights and the nature of permitted use of copyright material under the Copyright Act.'

398 As counsel for Mr Rose noted, the first published draft Bill included the provision that is now s 112E, but with the word 'facilities' qualified by the word 'physical'. That qualification was abandoned in the final Bill. In his Second Reading Speech to the Bill, the then Attorney-General said:

'The amendments in the bill also respond to the concerns of carriers and carriage service providers, such as Internet service providers, about the uncertainty of the circumstances in which they could be liable for copyright infringements by their customers. The provisions in the bill limit and clarify the liability of carriers and Internet service providers in relation to both direct and authorisation liability. The amendments also overcome the 1997 High Court decision of APRA v Telstra in which Telstra, as a carrier, was held to be liable for the playing of music-on-hold by its subscribers to their clients, even though Telstra exercised no control in determining the content of the music played.

Typically, the person responsible for determining the content of copyright material online would be a web site proprietor, not a carrier or Internet service provider. Under the amendments, therefore, carriers and Internet service providers will not be directly liable for communicating material to the public if they are not responsible for determining the content of the material. The reforms provide that a carrier or Internet service provider will not be taken to have authorised an infringement of copyright merely through the provision of facilities on which the infringement occurs. Further, the bill provides an inclusive list of factors to assist in determining whether the authorisation of an infringement has occurred.'

399 A statutory provision to the effect that a person is not to be taken to have authorised an infringement merely because another person does a particular thing leaves open the possibility that, for other reasons, the first person may be taken to have authorised the infringement. Such a provision does not confer general immunity against a finding of authorisation. Consequently, s 112E does not preclude the possibility that a person who falls within the section may be held, for other reasons, to be an authoriser. Whether or not the person should be so held is to be determined, in the present context, by reference to s 101 of the Act.

(iv) The application of s 101 to Sharman and Sharman Holdings

400 It is convenient to say immediately that I see no basis upon which it may be held that Sharman Holdings has authorised any infringements of copyright (or, indeed, committed any of the other infringements and breaches of duty alleged against it). The evidence provides little information about Sharman Holdings. All that is revealed is the date and place of the company's incorporation and the name of its sole director and sole shareholder. It is not shown to have done any particular act. It is possible that, as its name suggests, Sharman Holdings does no more than hold assets used by others. Insofar as it relates to Sharman Holdings, the proceeding must be dismissed.

401 The situation in relation to Sharman is different, at least in respect of authorisation. Sharman is the operator of the Kazaa system. As I have said, Sharman falls within s 112E. Sharman is not to be held to have authorised copyright infringement by Kazaa users merely because it provides the facilities they use in order to infringe the applicants' copyright. Something more is required. In evaluating the 'something more', regard must be paid to the factors listed in s 101(1A) of the Act, but bearing in mind Tamberlin J's observation in *Cooper*, that this is not an exhaustive list.

402 I accept that the intention behind the addition of s 101(1A) to the Act was to elucidate, rather than to vary, the pre-existing law about authorisation. I further accept, as did Bennett J in *Metro*, the continuing applicability of the *Moorhouse* test. A claim of authorisation can be made good only where it is shown that the person has sanctioned, approved or countenanced the infringement. It is not essential there be direct evidence of the person's attitude; as Gibbs J said in *Moorhouse*, inactivity or indifference, exhibited by acts of commission or omission, may reach such a degree as to support an inference of authorisation or permission.

403 Although s 112E provides that the provision of facilities is not enough to constitute authorisation, such provision is a matter relevant to 'the nature of [the] relationship' between Sharman and Kazaa users. If Sharman had not provided to users the facilities necessary for file-sharing, there would be no Kazaa file-sharing at all.

404 At all material times, it has been in Sharman's financial interest for there to be ever-increasing file-sharing, involving an ever-greater number of people. Sharman always knew users were likely to share files that were subject to copyright. At least since the Syzygy report in May 2003, Sharman, through Ms Hemming and Mr Morle, have been aware this was a major, even the predominant, use of the Kazaa system.

405 In the present case, the applicants are able to point to evidence of positive acts by Sharman that would have had the effect of encouraging copyright infringement. These acts include:

> (i) Sharman's website promotion of KMD as a file-sharing facility: see paras 68, 71, 73, 74, 78 and 79;
> (ii) Sharman's exhortations to users to use this facility and share their files: see paras 69, 77, 80 and 81;
> (iii) Sharman's 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: see paras 81-84 and 178. 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.

406 Importantly, these acts took place in the context that Sharman knew the files shared by Kazaa users were largely copyright works.

407 It is true, as the respondents emphasised, that Sharman's promotional statements were made against the background that each page of the Kazaa website, contained a notice, albeit in small print, that Sharman does not 'condone activities and actions that breach the rights of copyright owners'. It is also true that users were told about the relevant EULA and made to click a box whereby they agreed to be bound by the EULA. 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. That report showed the notices and EULA had had no effect on the behaviour of the focus group participants. As the participants were selected on the basis that they were representative of Kazaa users as a whole, or at least of young Kazaa users, those directing the affairs of Sharman (and Altnet) could not have done otherwise than appreciate that, notwithstanding what was on the website, copyright infringement was rife. Despite this, Sharman took no steps to include a filtering mechanism in its software, even in software intended to be provided to new users. There is no credible evidence that filtering was ever discussed. Sharman did not withdraw the 'Join the Revolution' material from its website. Rather, it included that material in the later version 3.0.

408 There is no evidence to suggest Ms Hemming, Mr Morle, Mr Bermeister or Mr Rose ever confronted the inconsistency between Sharman's website statements about not condoning copyright infringement and its conduct in the face of knowledge about what was actually happening.

409 Paragraphs (a) and (c) of s 101(1A) require consideration of the extent of Sharman's power to prevent copyright file-sharing and the steps it took to prevent or avoid that practice, including compliance with any relevant industry code of practice. There is no evidence of the existence of any such code.

410 The notices posted on Sharman's website about copyright infringement and the EULA are relevant to paras (a) and (c). However, the evidence shows that, to the knowledge of Sharman, they failed to prevent widespread copyright infringement.

411 If I am correct in my conclusions about keyword filtering (paras 254 to 294 above) and gold file flood filtering (paras 310 to 330 above), Sharman had power (in the case of gold file flood filtering, in conjunction with Altnet) to prevent, or at least substantially to reduce, the incidence of copyright file-sharing. Yet Sharman did nothing; even when it introduced KMD v3 one week before commencement of the trial of this proceeding.

412 Counsel for the Sharman respondents argued that Kazaa users did not 'make a copy of the sound recording', within the meaning of s 85(1)(a) of the Act, merely by downloading a shared file into their computers. The argument was based on the proposition that the downloaded material would not fall within the definition of 'record' in s 10(1)(e) of the Act. I question whether that proposition is correct. However, it is not necessary to reach a conclusion about it. The function of s 10(1) is merely to indicate the meaning, in the Act, of particular words. The word 'record' is not used in s 85, so the defined meaning of that word is irrelevant to the interpretation of that section.

413 The word 'copy' is not relevantly defined by the Act. However, in normal parlance, it covers the digital transmission of the aggregate of sounds contained in a sound recording into a computer's data storage system, enabling those sounds to be reproduced at will or to be passed on to someone else.

414 Counsel for the Altnet respondents argued it would not be possible to find authorisation unless I was satisfied that Sharman was in a position to 'control' the file-sharing behaviour of Kazaa users. 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. However, it would not be inapt to use the word 'control' to describe Sharman's position. Sharman was not able to control the decisions of individual users

as to whether or not they would engage in file-sharing and, if so, which particular works they would place into their 'My Shared Folder' file or download from other people. However, 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. Sharman did not do so; with the result that the relevant applicant's copyright in each of the Defined Recordings was infringed.

415 There is no evidence as to the identity of the particular Kazaa user or users who made available for sharing, or downloaded from another user, each of the Defined Recordings. However, somebody must have done so. Witnesses for the applicants gave uncontested evidence of being able to download each of these sound recordings as blue files.

416 Counsel for the Amici argued that to require software providers 'to monitor content for infringement would be wrong (because of eg. ss 22(6) and 112E, evidencing Parliament's intent to "protect the messenger"), unrealistic and unfair.' Counsel said '[t]his would shift, without justification, the burden of enforcement away from the rights holder and onto unrelated third parties ... and remove from the rights holder any motivation to protect its own property ... and would fail to promote new technologies'.

417 The last point echoes a complaint of counsel for the Altnet respondents about the applicants' decision 'to release music on open CD format (in contrast with the secure DRM protected, gold files distributed by Altnet)' and the fact that some of the applicants, or their associates, market appliances that enable people to 'rip' CDs.

418 I accept that Parliament intended to 'protect the messenger', although only to the extent indicated by the Act; notably s 112E. However, on my findings, Sharman is and was more than a 'messenger'. Whether it is 'unrealistic and unfair' that a software provider in Sharman's position should be held to have authorised copyright infringement by users of the software is a matter of opinion. The Court must take guidance from the Act, as elucidated by relevant judicial decisions. It is not for the Court to reject that guidance on the basis that the particular judge considers the result to be unrealistic and unfair. If Parliament thinks that is, indeed, the result of applying the Act, the remedy is in its hands.

419 The available evidence does not permit me to reach any clear conclusion as to the steps that might have been available to the applicants directly to protect their copyright in works reproduced in CDs distributed by them. The reason that evidence was not adduced, I surmise, is that all the respondents' counsel realised it is not a defence to an action for copyright infringement for a respondent to point to failings in self-protection by the copyright owner. Copyright law contains no equivalent of the doctrine of contributory negligence. If counsel are correct in asserting the applicants could have achieved some protection by adopting a DRM format, the applicants might do well to consider taking that course. However, neither the assertion nor the applicants' reaction to it can affect the legal issues now before the Court.

420 In my opinion, having regard to the whole of the relevant evidence, it should be held that Sharman infringed the applicants' copyright in their respective Defined Recordings by authorising Kazaa users to make copies of those sound recordings and to communicate those recordings to the public. By maintaining the Kazaa system in its present form, Sharman threatens to infringe the applicants' copyright in their other sound recordings in the same way.

(v) The application of s 101 to LEF and Ms Hemming

421 LEF is wholly owned and controlled by Ms Hemming. It is a 'one-woman' company, Ms Hemming's *alter ego*. Consequently, no distinction should be made between the position of these two respondents.

422 Counsel for the Sharman respondents disputed that any of their clients authorised copyright infringement by Kazaa users. However, they also argued that, in any event, Ms Hemming should not be made liable for any authorisation by Sharman. They referred to an observation by Gummow J in *Hanimex* at 283:

> *'Where the infringer is a corporation questions frequently arise as to the degree of involvement on the part of directors necessary for them to be rendered personally liable. Those questions are not immediately answered by principles dealing with "authorisation" or joint tortfeasance. Rather, recourse is to be had to the body of authority which explains the circumstances in which an officer of a corporation is personally liable for the torts of the corporation.'*

423 Gummow J went on to cite several cases. I need not deal with those cases. There is more recent authority on the point.

424 In *King v Milpurrurra* (1996) 66 FCR 474 at 494, Beazley J said:

> *'It will be recalled that in* [Hanimex]*, Gummow J stated that the principles dealing, inter alia, with joint tortfeasance, did not directly apply when determining whether a director was liable for a company's infringement of copyright. This must be so. The essence of joint tortfeasance is "concerted action to a common end":* The Koursk *[1924] P 140 at 156. This notion does not fit easily with the liability of a director for the company's wrongs. This is because, as Lord Reid said in* Tesco Supermarkets Ltd v Nattrass *[[1972] AC 153] at 170-171, the person who is the directing mind and will of the company:*
>
> *"is an embodiment of the company ... and his mind is the mind of the company ... Normally, [a] board of directors ... carry out the functions of management and speak and act as the company."*
>
> *It follows that the principles to consider are those relating to the personal liability of a director for the tortious conduct of the company.'*

425 Beazley J said that, notwithstanding the separate legal existence of a company, 'it has long been recognised that a director may be liable for a tortious act committed by the company'. However, she remarked, 'the authorities differ as to the principles which govern a director's liability in such a case'.

426 Beazley J identified two competing lines of authority: cases that held 'a director is personally liable for a tortious act committed by the company which the director has ordered or procured to be done' ('the *Performing Right Society* test') and cases that applied a higher test ('the *Mentmore* test'), whether the director (or officer) made 'the tortious act his own'. Although Beazley J acknowledged that the test usually applied in Australian intellectual property cases was the *Performing Right Society* test, she thought that test was unsatisfactory; it failed to 'pay sufficient regard, either to the separate legal existence of the company, or to the fact that the company acts through its directors'. Her Honour preferred the *Mentmore* test.

427 In *Microsoft Corporation v Auschina Polaris Pty Ltd* (1996) 71 FCR 231 ('*Auschina Polaris'*) at 239, Lindgren J also accepted the statement of principle of Gummow J in *Hanimex*. He went on to refer to the

conflict of authority discussed by Beazley J, but he preferred the *Performing Right Society* test.

428 The same issue was discussed, in the context of a claimed patent infringement, by Finkelstein J in *Root Quality Pty Ltd v Root Control Technologies Pty Ltd* [2000] FCA 980; 177 ALR 231 (*'Root Quality'*).

429 Finkelstein J rejected the *Performing Right Society* test. He thought it presented a number of difficulties. At [125], his Honour said:

> *'The first arises from the nature of corporate personality and the liability of a corporation for the acts of its agents. A corporation is an abstraction; a creature of statute. It can carry out acts only because the law attributes to the corporation certain actions of its directors and officers. Thus a corporation can interfere with the rights of a third party only when the acts constituting the unlawful interference are attributed to the corporation. There is a reason why, in that circumstance, the law should not impose liability both on the corporation for unlawful interference and separate liability on the director or officer for procuring that interference.'*

430 On the other hand, Finkelstein J was uncomfortable with the *Mentmore* line of cases under which, he thought, 'it would not always be easy to identify the circumstances under which a director could "make that tort his own".' He concluded, at [146]:

> *'All that can be said confidently is that if a director decides that his company should carry out an act that results in an infringement of the rights of a third party, the director does not, without more, render himself personally liable at the suit of the third party ... The director's conduct must be 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. If a director deliberately takes steps to procure the commission of an act which the director knows is unlawful and procures that act for the purpose of causing injury to a third party, then plainly it is just that liability should be imposed upon him. Lesser conduct may suffice. For example, if the director is recklessly indifferent as regards whether his company's act was unlawful and would cause harm, that may also suffice. In the end it will depend upon the facts of each particular case. Where the boundary lies, between the non-tortious conduct of a director who acts* bona fide *within the course of his authority and the tortious conduct of a director who acts deliberately and maliciously to cause harm, cannot be stated with any precision.'*

431 The issue of the proper test was inconclusively noted in two recent Full Court judgments. In *Allen Manufacturing Co Pty Ltd v McCallum & Co Pty Ltd* [2001] FCA 1838; 53 IPR 400, at [43] – [44], the Court said:

> *'The difference between the two tests may be more apparent than real. We are not aware of any case in which it has been held that a director or officer of a company directed or procured the company's infringing act, yet that person escaped liability because he or she did not deliberately, wilfully or knowingly pursue a course of conduct that was likely to constitute infringement or that reflected indifference to the risk of infringement. This may be because, in practice, an act of direction or procurement will generally meet the* Mentmore *test. It is notable that, in* Mentmore *itself, the Canadian Federal Court of Appeal declined (at 204) to "go so far as to hold that the director or officer must know or have reason to know that the acts which he directs or procures constitute infringement". The Court declined to do this because that "would be to impose a condition of liability that does not exist for patent infringement generally".*

> *To the extent there is a real difference between the tests, each has eloquent supporters. One day it may be necessary, in a practical sense, to choose between them. But it is not necessary to do so in this case'*

432 In *Sydneywide Distributors Pty Ltd v Red Bull Australia Pty Ltd* [2002] FCAFC 157 at [160] – [161], Weinberg and Dowsett JJ mentioned the two lines of authority. However, the issue went off on a pleading point.

433 It will be apparent that the authorities are in some disarray. There are numerous cases, some of them recent, that would support a decision to adopt the *Performing Right Society* test and ask whether Ms Hemming procured and directed the acts and omissions of Sharman that constituted authorisation of users' infringements of the applicants' copyrights. There could be only an affirmative answer to that question.

434 However, in recent years, several members of this Court have expressed dissatisfaction with the *Performing Right Society* test and have argued for the adoption of something more rigorous. Some judges have favoured the *Mentmore* test and asked whether the person 'made the tort his own'. My difficulty is that, like Lindgren J in *Auschina Polaris* and Finkelstein J in *Root Quality*, I am not sure what that test means. Like their Honours, I prefer to eschew any catchphrase and consider the justice of the case. In *Root Quality*, Finkelstein J said: 'The director's conduct must be 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'. I am happy to adopt that test, with the qualification that the person need not be a director of the company. I adopt that approach the more readily because I believe it encapsulates the approach which has in fact been taken, although perhaps not articulated in those words, in many intellectual property cases in this Court. See, for example, *Jain* at 53; *Auschina Polaris* at 246; *Metro* at 593; and *Cooper* at [130].

435 Jain is particularly interesting. In that case the Full Court imposed personal liability for 'a studied and deliberate course of action in which Mr Jain decided to ignore the appellant's right and to allow a situation to develop and to continue in which he must have known that it was likely that the appellants' music would be played without any licence from it. It was within his power to control what was occurring be [sic] he did nothing at all'.

436 It is not in dispute that Ms Hemming is CEO of Sharman and that she directs LEF's performance of its obligations under its management services agreement with Sharman. Counsel for the Sharman respondents cited evidence from Mr Morle that, in November 2004, a total of 19 persons were involved in running Sharman's business. However, as counsel for the applicant noted, Ms Hemming has always been the person in charge of Sharman's affairs. She and Mr Morris, who was second-in-charge and then in London, were the only people working for Sharman when Mr Morle was engaged in January 2002.

437 Counsel for the Sharman respondents emphasised there exists a Sharman executive committee which meets to address management and other issues as they arise. Counsel also pointed out the Kazaa file-sharing system existed before Ms Hemming was introduced to it by Mr Bermeister. There had been a relationship between BDE and Kazaa BV before Ms Hemming became involved.

438 In submissions in reply, counsel for the applicants emphasised that their clients' case against Ms Hemming was not confined to her role as director of LEF. They contended she personally authorised the infringing acts and entered into a common design with, or induced, the Altnet parties to authorise copyright infringements.

439 Ms Hemming has been intimately involved in the activities of Sharman from the time of its incorporation. It is true that she has been assisted by others and that there is an executive committee; although we know little about its activities. Presumably the executive committee discusses controversial issues. Perhaps, it makes collective decisions concerning actions to be taken, and not to be taken, by Sharman. However, Ms Hemming is 'the boss'; Mr Morle made that clear. 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.

440 Although Ms Hemming is apparently not a highly-qualified technical person, it is apparent from the documentary evidence that she has always had a good understanding of the Kazaa technology. She has always been aware of the file-sharing feature of KMD and, at least since May 2003, that the manner in which this feature is habitually used involves widespread infringement of copyright. Although Ms Hemming was in charge of Sharman, and had a close working relationship with officers of Altnet (including Mr Bermeister), she did nothing to curtail that infringement.

441 The Kazaa system commenced to operate before Ms Hemming became involved. The system may not have been the same at that stage. In the course of a lengthy answer to a question asked by Mr Bannon, Professor Tygar made a revealing comment. He said:

> *'I used Kazaa before it was acquired by Sharman and I believed that, at that time, there was a Kazaa server but in version 1.5, which was the first version that Sharman released afterwards, there was no Kazaa server.'*

That evidence suggests a significant change in the structure of the system, in a direction away from ability to control users' activities, after the system came under the management of Ms Hemming.

442 The answer to interrogatories of Ms Hemming, quoted at para 97 above, suggests her relationship to Sharman might be more than simply a CEO supplied under a management services agreement. Ms Hemming recounted how Mr Bermeister told her that 'Kazaa BV was looking to sell its assets'. She said Mr Bermeister spoke about the nature of the Kazaa system and the relationship between Kazaa BV and Altnet. She went on:

> *'He offered to introduce me if I was interested in buying any assets. In a subsequent conversation I asked him to introduce me to Kazaa BV.'*

443 In the absence of any explanation from Ms Hemming, I interpret this answer as indicating that Ms Hemming sought the introduction because she was interested in buying Kazaa BV's assets; that is, the Kazaa system. In other words, she wished to be a principal, not a mere consultant or employee. The inference that Ms Hemming was herself the purchaser of the Kazaa system (either alone or with others) is supported by her claim, in the answer to interrogatories, that 'there were no investors'.

444 In their submissions in reply, counsel for the applicants submitted I should adopt the *Performing Right Society* test. However, they recognised the relevant question will always be the extent of the involvement of the particular company director (or officer) in the infringing conduct. The thrust of counsel's submission is that liability has been imposed on individual directors or officers who have been shown to have been personally involved, in a deliberate and continuing way, in the company's authorisation of infringing conduct.

445 In the present case, it may be open to the Court to do more than find that Ms Hemming, having the power to control what was happening, did nothing at all. A combination of the two possible inferences suggested above would lead to a conclusion that Ms Hemming (alone or with others) purchased the Kazaa system from Kazaa BV and then caused, or allowed, its structure to be changed away from the use of a Kazaaserver; presumably, to enable Sharman to argue (as it has done in this case) that it has no control over the copyright infringing conduct of Kazaa users.

446 In the absence of rebutting evidence on either of the points, I am inclined to the view that I should reach that conclusion. However, it is not necessary to determine that matter. At the very least, the case is on all fours with *Jain*. See also *Auschina Polaris* at 246 and *Metro* at 593.

447 LEF and Ms Hemming should be held to have authorised the Kazaa users' infringements of copyright in the applicants' sound recordings.

(vi) The application of s 101 to Mr Morle

448 Similar questions of principle arise in connection with Mr Morle's part in Sharman's acts and omissions. However, in his case, the questions demand a different answer. Mr Morle was aware of the fact that Kazaa users habitually shared copyright material, including sound recordings. Mr Morle did nothing to prevent or reduce that activity, notwithstanding that, as Sharman's Director of Technology, Mr Morle was well-placed to take the lead in dealing with the problem of copyright infringement. The design and development of KMD was one of his responsibilities. He liaised with other parties (Joltid, Bluemoon and Altnet) on that subject. Yet he did nothing about developing the capacity to filter users' copyright-infringing requests. Either on instructions or of his own volition, Mr Morle turned a blind eye to the issue.

449 However, the 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. According to Mr Morle, he is, and always has been, a mere employee of LEF seconded to Sharman; he has never had a financial interest in Sharman. There is no material that rebuts, and I see reason to reject, this evidence.

450 Mr Morle is not, and never has been, in control of Sharman. His position has always been subservient to that of Ms Hemming. I have no reason to believe that, if Mr Morle had wished to take steps to prevent, or reduce the incidence of, file-sharing copyright infringement, his wish would have prevailed. On the contrary, having regard to the economic realities, I suspect, had Mr Morle aired such a wish, he would soon have been looking for a new job.

451 It should be concluded that Mr Morle did not authorise Kazaa users' copyright infringements.

(vii) The application of s 101 to the Altnet companies

452 The applicants do not contend that any of the Altnet companies directly operate the Kazaa system. However, they say these companies each authorise Kazaa users' infringement of copyright because their business is 'extremely closely aligned if not inextricably linked', to that of Sharman.

453 In assessing that submission, it will be necessary to refer to a number of evidentiary matters. However, before doing so, I should make reference to the separate positions of each of the three Altnet companies.

454 Altnet is the operator of the Altnet system. As mentioned at para 109 above, since its formation, Altnet has been jointly owned by BDE and Joltid. BDE is the majority shareholder. Mr Bermeister, the President and CEO of BDE, has always been the sole director of Altnet. It is reasonable to treat Altnet as being controlled by Mr Bermeister primarily on behalf of BDE. As BDE expressed the situation in its report to the SEC for the fiscal year of 2003 ('the SEC report'): '[BDE] is a company which, through [Altnet], operates a peer-to-peer based content distribution network that allows us to securely and efficiently distribute a content owner's music, video, software and other digital files to computer users via the Internet.'

455 Having regard to BDE's control of Altnet, it should be held that the actions of Altnet are actions of BDE. If Altnet is liable for copyright infringement, so is BDE.

456 At para 110, I noted that little is known of BDE Pty Ltd. The directors of BDE Pty Ltd are Mr Bermeister and Mr Miller, both directors of BDE. BDE Pty Ltd apparently occupies premises in Surry Hills, Sydney. Those premises may be used in connection with the operation of the Altnet system, but there is no evidence about that matter. There is insufficient material to enable me to conclude that BDE Pty Ltd is implicated in authorisation of the applicants' copyright. Nor is there material establishing any other wrongful conduct by this respondent. The proceeding must be dismissed, as against BDE Pty Ltd.

457 The applicants argued the Kazaa system is a joint venture between Sharman and Altnet under which Sharman provides the FastTrack peer-to-peer technology and Altnet supplies the TopSearch licensed file technology; the two systems are closely integrated and the two companies' interests are interdependent.

458 Although the SEC report revealed that Altnet had recently made agreements with other peer-to-peer file-sharing companies, Sharman was there stated to be 'our largest distributor and source of over 90% of our revenue'. Reference was made to Altnet's joint enterprise agreement with Sharman: see para 113 above. As there stated, that agreement recited that Sharman 'was created with the intention of working jointly with Altnet to develop a business by which the power of peer-to-peer file-sharing could be used to distribute copyright licensed content to profit'. Note the reference to 'a' business, in the singular, and the terms of the joint enterprise agreement which, effectively, give Altnet a high degree of control over the Kazaa system.

459 At para 121 above, I set out other features of the Sharman-Altnet relationship noted by counsel for the appellants. I need not repeat those points. They were not put into dispute. They provide support for counsel's submission that the Kazaa system is conducted as a joint venture between Sharman and Altnet.

460 The primary submission of counsel for the Altnet respondents was that Sharman had not violated the applicants' rights; it had not authorised Kazaa users' infringements of copyright. Alternatively, however, counsel sought to distance their clients from Sharman. In their Closing Submissions, counsel said:

> *'[T]here is no dispute that there is a commercial relationship between the companies. There is no dispute that BDE's revenue is predominantly derived from its software being made available to KMD users. There is no dispute that, at the technical level, there is liaison between the programmers at Sharman and those at BDE, nor that the KMD is designed to be distributed with, and executed concurrently with, the "Altnet Technology". There is no dispute that there are personal relationships between the officers of the groups of companies. Those matters, of course, make the Sharman/BDE relationship similar to thousands of other affiliations of corporations whose interests, in part, converge, and it would be surprising if anything else were the position.*

But that does not mean that the distinct corporate personalities are a sham or that in reality there is a "joint enterprise" conducted as "a single unit" such that the Court can ignore the separate identities of the respondents ... It is plain that:

(a) first, the interests of Sharman and BDE do not always coincide, and from time to time have been opposed;
(b) secondly, BDE has business relationships with third parties, some of which are Sharman's direct competitors;
(c) thirdly, BDE Inc pre-dates Sharman (and, for that matter, the KMD) and has a long history of manufacturing and distributing content on personal computers;
(d) fourthly, there is the simple matter of geography: most of BDE Inc's board of directors, most of its stockholders, and the overwhelming majority of its revenue and expenses, are located in the United States. The geography alone is a considerable obstacle to the applicants' "single unit" theory. It is to be remembered that, at the time the alleged conspiracy is said to have been formed, Mr Bermeister was in the United States.'

461 In the face of the documentary evidence, these protestations are unpersuasive. Whether the Sharman-Altnet relationship is similar to, or different from, other commercial relationships is immaterial. The question is whether this relationship is such that it must be said the acts and omissions of Sharman, in relation to the authorisation of users' copyright infringement, are also acts and omissions of Altnet and BDE. The fact that the interests of two parties do not always coincide does not negate the possibility that those parties may be engaged in a joint venture, or partnership, in respect of a particular activity or series of activities. It is immaterial that other interests of the joint venturers may be unshared, even conflicting.

462 It is true that BDE pre-dated Sharman; even the creation of the Kazaa system. However, Altnet was formed within weeks of the incorporation of Sharman. From the date of its incorporation, Altnet's sole director was Mr Bermeister, a person who had already had a working relationship with Ms Hemming and who knew of her entry into the area of peer-to-peer file sharing.

463 The 'simple matter of geography' is singularly unconvincing in an age of instant global communication. Geography provides no reason to reject the possibility of a joint venture between American and Australian interests.

464 The documentary evidence is full of examples of consultation and close co-operation between officers of Altnet (including Mr Bermeister and Mr Rose) and officers of Sharman (including Ms Hemming and Mr Morle). The consultation and co-operation embraced a wide range of matters, from broad policy formation to operational details. Graphic evidence of Altnet's involvement in the Kazaa system is provided by the fact that it was Altnet (not Sharman) which proposed the commissioning of Syzygy to conduct focus groups and that Mr Bermeister took the time to attend all four focus group discussions and to report his observations to others, including Ms Hemming and Mr Morle. It is plain that Altnet had a lively, ongoing interest in the operation of the Kazaa system and its profitability.

465 Although the gold files supplied to the Kazaa system by Altnet through TopSearch are assumed all to have been non-infringing files, Altnet knew this was not the case with the KMD blue files. Altnet knew there was substantial copyright infringement in this area. Notwithstanding that knowledge, it took no steps to prevent or avoid users' copyright infringements. In particular, it took no steps to take advantage of what BDE said in the SEC report was 'its ability to communicate with the KMD technology'. BDE went on:

> *'The KMD permits end users to exchange files with other KMD users over the Fasttrack network. Tens of millions of search requests each day are being made using the KMD by users worldwide. These search requests can be accessed by Altnet, and pursuant to our agreement with Sharman Networks, relevant Altnet search results are displayed in the KMD to end users in response to their search requests.'*

466 As noted at paras 312-313 above, Mr McKemmish agreed this technology would have enabled Altnet to respond to a request for a listed unlicensed work by flooding the user's screen with empty gold files. Altnet did not take advantage of that capacity, no doubt because that would have been contrary to its financial interests.

467 The joint enterprise agreement is very persuasive. Not only does it recite the fact that Sharman was created with the intention of working jointly with Altnet to develop the Kazaa business (para 113 above), it grants Altnet a licence to use Sharman's name, trademarks and logos (para 116) and provides for the sharing of search results (para 117) and revenue (para 119). Moreover, Altnet has the right, and ability, to monitor users' KMD searches and to impose its gold file offers on the Kazaa UI. This looks like a business partnership. That this is the way Altnet (and BDE) saw the relationship is apparent from the SEC report quoted at para 133 above.

468 I see no reason why I should not take the joint enterprise agreement at face value and find that Altnet is a co-principal, with Sharman, in the provision of the Kazaa system to members of the public. Such a finding is not inconsistent with the other documentary evidence or Mr Morle's evidence. On the basis that Altnet and Sharman jointly provide Kazaa, Altnet is a person to whom s 112E of the Act applies. Altnet 'provides facilities', in conjunction with Sharman, within the meaning of that section. However, on the stated basis, Altnet does more than provide facilities for making, or facilitating the making of, a communication. It is involved in Sharman's additional activities.

469 Moreover, Altnet has made its own contribution to Kazaa. As Mr Morle explained, one of his first tasks was to rebuild the Kazaa website. Shortly afterwards, he added TopSearch to KMD. He did this in collaboration with Mr Rose. They installed the promotional features that persuade me that Sharman did more than provide facilities able to be used by copyright infringers: see para 403 above. Altnet must have known about those features. During the time that he was installing the features, Mr Morle was working in close collaboration with Mr Bermeister and Mr Rose. Altnet seems to have taken a close interest in everything Mr Morle did. For example, an undated document entitled 'The Altnet Research Network – Sharman Networks Planning Document' makes this specific reference to the Kazaa website:

> *'**Kazaa.com promotion***
> *The web site is becoming a positive educational and promotional tool, with reasonable integrity and trust. We will preview, review and educate customers through the various stages of the launch. This information has to be plain language, including both clear summaries and comprehensive detail. Preview ('coming soon') information should be placed on the site long enough to allow reference groups to debate and discuss the issues and feel comfortable with trying the new product.'*

470 A specific example of consultation in relation to the Kazaa website is provided by an exchange of emails in September 2003. On 3 September, Mr de Re of Sharman sent to Mr Bermeister an email headed 'URGENT. Feedback required'. The email commenced:

> *'As you know we are working on the redesign of the KMD interface. I have collated form [sic] SNL and Altnet a list of requirements for what the interface needs to achieve. I would be grateful if you could prioritise this list starting from what you think are the most important objectives down to the least. I will then pass this on to Nikki for final approval before the design is executed.'*

Then followed a list of objectives of the redesign and a request for feedback.

471 Two days later, Mr Bermeister provided his own list of desirable features of the website. He did not mention warnings about copyright infringement.

472 Altnet is implicated, equally with Sharman, in the conduct that causes me to find that Sharman authorised Kazaa users to infringe the applicants' copyright.

473 The issue of authorisation should be resolved adversely to Altnet and BDE.

(viii) The application of s 101 to Mr Bermeister

474 It is not necessary for me to rediscuss the principles that are relevant to determination of the question whether Mr Bermeister should be held to have personally authorised users' infringement of the applicants' copyright, as distinct from having done this on behalf of Altnet and BDE. There is no doubt that Mr Bermeister procured and directed the acts and omissions of Altnet and BDE which, I have concluded, require a finding that those companies authorised the infringements. However, as in the cases of Ms Hemming and Mr Morle, I prefer to adopt the more demanding test postulated by Finkelstein J in *Root Quality*.

475 I think Mr Bermeister's degree of personal involvement in Altnet's and BDE's authorising conduct was such as to make it just that he be rendered liable for infringement of the applicants' copyright. Altnet is not a 'one-man' company, in the sense that it is owned by one person. It is owned by BDE and Joltid, with BDE having the majority of the issued shares. However, since its formation, Mr Bermeister has been the sole director of Altnet. No doubt he has exercised his powers in accordance with the best interests of the shareholders. Nevertheless, Mr Bermeister has enjoyed total control over Altnet's management. The major activity of the company – perhaps its only activity – has been the establishment, maintenance and expansion of the Altnet file-licensing system. A dominant aspect of that activity has been Altnet's relationship with Sharman and Altnet's participation in the Kazaa system.

476 Moreover, as will be apparent from the material already mentioned, Mr Bermeister himself has played a key role in the Altnet-Sharman relationship. It seems he was instrumental in creating that relationship. He introduced Ms Hemming to Kazaa BV. In a manner left unexplained by the evidence, this led to the incorporation of Sharman and its entering into agreements with Kazaa BV and Joltid. Altnet then made a joint venture agreement with Sharman. The combined effect of these various agreements was to enable Sharman to operate the Kazaa system. It was apparently always envisaged that Altnet's TopSearch technology would be part of the Kazaa system. Mr Bermeister was personally involved in ensuring this would be so.

477 Mr Bermeister was not content merely to set up the Sharman relationship and to cause the pooling of the relevant technologies. The documentary evidence shows he took a close personal interest in the operation of Kazaa. He offered opinions, or was consulted, about many operational matters, including the

content of the Kazaa website. He attended the focus groups, at which he must have come to realise, if he did not know before, the extent to which the Kazaa system was used for unauthorised file-sharing. Yet he did nothing about that problem. He allowed Altnet to remain in the relationship with Sharman, enjoying the profits of that relationship, without making even a suggestion as to how the incidence of unauthorised file-sharing might be reduced.

478 Mr Bermeister has always been only one of several BDE directors; although, as President and CEO, he may reasonably be assumed to have played an influential role in BDE's affairs. I assume it has been his practice regularly to report to the BDE board of directors, including in relation to Altnet's involvement in the Kazaa system. However, there is no suggestion in the evidence that any of his actions and omissions, in relation to Altnet and the Kazaa system, were forced upon him by the board. In the absence of evidence to the contrary, from Mr Bermeister or anyone else in BDE/Altnet, it may be inferred that Mr Bermeister is, and always has been, the driving force in relation to this area of BDE's activities, and that his fellow-directors have been content to allow him free rein.

479 In my opinion, the 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.

(ix) The application of s 101 to Mr Rose

480 The evidence provides little information about Mr Rose. In their Closing Submissions, counsel for Mr Rose made some assertions about his history and positions with BDE. I cannot act on those assertions; they are not supported by evidence. There is evidence as to the identity of the directors of BDE and Altnet; Mr Rose is not among them. So I can accept counsel's submission that he has never been a director of either company. It also appears to be correct, as asserted by counsel, that Mr Rose has never been named in a BDE report to the SEC as a 'key person' in its business. Apparently, at one stage, he was called 'Vice President of Technology'; later he became 'Chief Technology Officer'. Counsel also asserted that Mr Rose was located in Australia, remotely from BDE in America. However, there is no evidence about that. Nor is there any evidence to support counsel's assertions: first, that Mr Rose's role with BDE was limited to 'implementing the decisions of others'; and, second, that he had no connection with the establishment of Sharman or its acquiring the Kazaa business. All I can say about those two assertions is that there is no evidence contradictory of them.

481 Counsel also submitted that Mr Rose 'had no connection with [Sharman] except insofar as he was required to deal with persons working for that company in carrying out the duties of his employment with [BDE]'. That may be true; once again, there is no evidence to the contrary. However, if the statement is true, that is not enough to resolve the issue of his personal liability. It is still necessary to consider the evidence as to what he did in relation to the Sharman connection.

482 In a Schedule to their Closing Submissions, counsel for the applicants identified 59 documents, included in the evidence, that are connected in some way with Mr Rose. Counsel claimed these documents demonstrate that 'Mr Rose is deeply involved in the day to day management of [Altnet]'.

483 Counsel for the applicants went on to submit: 'Mr Rose had primary responsibility for technical issues in Altnet'. They identified 18 documents which, they claimed and I agree, support that statement. These documents show Mr Rose played a role in the design of TopSearch; that he collaborated with Mr Morle in the integration of the TopSearch and FastTrack technology; and that he was involved in monitoring and

improving the operation of the Kazaa system, including the design of upgrades and new versions. The documents also show that Mr Rose devoted attention to the collection of statistics. In short, the documents show what might be expected about someone in his position: Mr Rose was totally familiar with the technological aspects of the Kazaa-Altnet system. He was aware of the objectives of Altnet in connection with that system and he endeavoured to achieve those objectives.

484 However, counsel for the applicants went further. They said 'Mr Rose was involved in a wide range of business and marketing decisions'. In support of that assertion, they cited 15 documents. Those documents indicate Mr Rose's involvement in particular issues. However, leaving aside cases where he was a mere recipient of information – for example, Mr Bermeister's memo commenting on the focus groups – in each case, Mr Rose's involvement was limited to providing information or comment about a technical matter. He suggested changes to both TopSearch and the Kazaa website. However, he is not shown ever to have been involved in basic policy decisions.

485 During the course of his oral evidence, Mr Morle made several references to interaction with Mr Rose. Those references did not add anything to the impression that, in any event, is gained by perusing the 59 documents.

486 As counsel for the applicants submitted, the documents demonstrate that Mr Rose was aware of Kazaa users' widespread copyright infringing activity and that he took no steps to prevent copyright infringement.

487 The evidence is not sufficient to make out the applicants' case against Mr Rose. At all material times, Mr Rose occupied an important position in the BDE/Altnet organisation. He was deeply involved in the technological aspects of the Kazaa system. However, there is no evidence to suggest he 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. Although Mr Rose occupied a senior position, he was always subservient to Mr Bermeister. I have no reason to believe any proposal Mr Rose might have advanced about measures to deal with copyright infringement would have been implemented.

488 The authorisation claim against Mr Rose must fail.

(x) Conclusions on authorisation

489 I have found that three of the Sharman parties (Sharman, LEF and Ms Hemming) and three of the Altnet parties (Altnet, BDE and Mr Bermeister) authorised infringement of the applicants' copyright by Kazaa users. They did this both individually and as joint tortfeasors pursuant to a common design. There is no doubt as to the close collaboration of Sharman and Altnet in developing and operating the system, and the involvement in that collaboration of Ms Hemming and Mr Bermeister on behalf of LEF and BDE respectively.

490 The authorisation claim fails as against Sharman Network, Mr Morle, BDE Pty Ltd and Mr Rose.

VI THE TRADE PRACTICES ACT CLAIMS
(i) Misleading conduct

491 At para 47 above, I set out the particular false representations pleaded by the applicants in support of their claim that the respondent corporations infringed s 52 of the TP Act and s 42 of the FT Act.

492 In their Closing submissions, counsel for the applicants dealt with the first two representations together. The gist of these representations was the inability of Sharman, or anyone else, to exercise control over the nature, quality or content of files that can be made available for download, or that was downloaded, by Kazaa users. There is no doubt the representations were made. However, as counsel for the Sharman respondents pointed out, the representations were in a section of the Kazaa website Guide, headed 'Information for Parents', that dealt with 'adult or other offensive or age inappropriate content'. Considered in that context, the representations were not misleading.

493 The third representation was pleaded as stating: 'that a significant or substantial portion of the revenue generated via the Kazaa Software comes from payment for distribution of rights managed content'. However, the relevant website statement, in both v2.6 and v3.0, was that revenue comes from content (distribution of licensed material), advertising and sales of products and services. That statement was true.

494 There is also evidence that, in a media interview, Mr Morle answered a question as to Sharman's 'main revenue stream' by saying:

> *'Multiple revenue streams. But certainly advertising is an enormous one. It's getting very colourful [sic] now because of the content we're putting through, which is the Altnet system.'*

495 It is common ground that advertising provides a main revenue stream for the operators of the Kazaa system. Mr Morle probably exaggerated the proportion of Sharman's revenue that was attributable to Altnet content. However, there is no evidence as to the proportions of Sharman's revenue that emanates from particular sources. Contrary to an implication in the applicants' submissions, it was not incumbent on Sharman to adduce evidence 'to substantiate the proposition that licensed files represent their main revenue source'. It was for the applicants to establish that the statement was misleading. They have not done so.

496 The fourth pleaded representation is 'that all files containing rights management information appear as gold icons in version 2.6 of the Kazaa Software'. A statement to that effect would probably be untrue. However, as counsel for the Sharman respondents pointed out, the statement actually made in the Guide section of the website was the converse: 'All files marked with Gold icons are digitally rights managed ...'. That statement was true.

497 The fifth and sixth pleaded representations concerned the effect of a user's personal computer functioning as a supernode: this will not, or is unlikely to, noticeably affect the performance of the computer or increase the cost of its operation. The evidence does not establish that either of these representations was untrue.

498 The seventh representation pleaded by the applicants is: 'that a user of Kazaa Software may avoid liability by altering the file data or metadata relating to infringing files'.

499 The applicants' submission justifies this claim by referring to a statement on the Kazaa website about dealing with bogus, fake or illegal files. The existence of this statement does not make good the pleaded representation.

500 Finally, the applicants pleaded that the respondents had represented 'that a significant or substantial proportion of files made available for download or downloaded by users via the Kazaa Software are non-infringing files'.

501 Counsel for the applicants asserted the respondents have repeatedly made this representation. However, they failed to identify any evidence to that effect. Furthermore, as counsel for the Sharman respondents pointed out, there is no evidence as to the proportion of files made available for download by KMD that are non-infringing files. On the evidence, it would be impossible to say the statement, if made, was false.

502 The applicants also rely on s 51A of the TP Act, and s 41 of the FT Act, in claiming that, to the extent that the representations were made in respect of future matters, the corporate respondents did not have reasonable grounds for making them at the time they were made. The pleading ties these two claim to the eight particularised representations, none of which is a representation about a future matter. There is no merit in the claim under s 51A of the TP Act and s 41 of the FT Act.

(ii) Unconscionable conduct

503 The applicants pleaded that the Sharman companies each engaged in unconscionable conduct in connection with the supply, or possible supply, of goods or services and that the other respondents were knowingly concerned in that conduct. Paragraph 146 of the S of C particularised this allegation in the following manner:

> *'(i) At all material times the respondents knew that the primary use of the Kazaa Software involved the infringement of copyright in commercial sound recordings.*
>
> *(ii) In the course of the ordinary use and operation of the Kazaa Software, users of the Kazaa Software are exposed to liability for infringement of copyright or authorisation of infringement of copyright by other users of the Kazaa Software, whether by making available unauthorised digital music files from their own computers, or by reason of their computers operating as supernodes indexing unauthorised digital music files made available on the computers of other users of the Kazaa Software.*
>
> *(iii) Users of the Kazaa Software are contractually required to indemnify the suppliers of the Kazaa Software in respect of any infringements of copyright arising from their conduct, by reason of the terms of the Kazaa End User License.*
>
> *(iv) The respondents have taken steps to minimise their liability in respect of or otherwise distance themselves from the consequences of infringing uses of the Kazaa Software, including by the imposition on users of the Kazaa Software of the indemnity referred to in sub-paragraph (iii) above.*
>
> *(v) In supplying the goods or services pleaded above, the respondents knowingly exploit the practical difficulties faced by the applicants in detecting, monitoring and taking action in relation to infringements of copyright by users occurring by means of the Kazaa Software.'*

504 However, in their Closing Submissions, the applicants' counsel put a somewhat different case. They said:

> *'The applicants rely on two aspects of the conduct involved in the supply of those services.*

The first consists of the circumstances in which the respondents fuelled the use of Kazaa without delivering adequate warnings to consumers about the possible legal consequences to those consumers of the use of the system to distribute music files (i.e. infringing copyright and becoming personally liable) and simultaneously imposed indemnity obligations on those consumers in relation to any liability that the respondents may face.

The second aspect is the fact that knowing the special disability that the applicants would face in relation to the supply of their goods and services to consumers in an environment of substantial use of the Kazaa software by Kazaa users, the Kazaa operators continued to supply, operate and encourage the use of the Kazaa software without any steps being taken to minimise the impact on the applicants.'

505 Counsel for the Sharman respondents replied by denying their clients supplied goods or services to consumers. I agree they did not supply goods. I prefer to reserve my position in relation to services. Whether or not the Sharman respondents supplied services, I agree with their counsel that neither aspect of the unconscionable conduct claim can succeed.

506 The first aspect of the Sharman companies' conduct fails on the facts. The Kazaa website contained warnings about copyright infringement. The EULA was clear. These steps were substantially ineffective. However, that was not because users were not warned; it was because they were unwilling to allow the warnings to affect their behaviour. The fact that this unwillingness was encouraged by other material on the Kazaa website does not mean there were no warnings.

507 The second aspect complains of unconscionability, not towards the recipients of the supplied goods or services, but towards the present applicants. However, in *Monroe Topple & Associates Pty Ltd v Institute of Chartered Accountants in Australia* [2002] FCA 197 at [116], Heerey J (with whom Black CJ and Tamberlin J agreed) held that s 51AC of the TP Act is not concerned with the impact of conduct on third parties. The wording of the relevant portions of s 51AB and s 51AC is almost identical, so this statement must also be true of s 51AB.

508 The unconscionable conduct claims must fail.

509 There is no merit in any of the TP Act or FT Act claims. The claims were not well thought-out. It would have been preferable if the applicants had refrained from further burdening an already heavy case by including these claims.

VII THE CONSPIRACY CLAIMS

510 The applicants pleaded that, on a date or dates unknown to the applicants, one or more of the respondents agreed with one or more of the other respondents to develop (or further develop), promote, distribute and operate the Kazaa system and that the predominant purpose of the agreement was to injure the first to sixth and eighteenth applicants. The applicants alleged it was part of the agreement that unlawful means would be used to effect that injury. The applicants claimed this agreement was carried out and has caused loss to the applicants.

511 In their Closing Submissions, counsel for the applicants made clear that they advanced two alternative bases for their conspiracy claim: conspiracy to injury and conspiracy by unlawful means. It is necessary to give separate consideration to these two alternatives.

512 Conspiracy to injure involves three elements:

> (i) an agreement between the alleged conspirators, not necessarily a legally enforceable agreement. The agreement may be an agreement which individual conspirators can join or leave from time to time;
> (ii) that the predominant purpose of the agreement was infliction of injury upon a particular person or persons; and
> (f) that the agreement was carried into effect, and thereby caused damage to that person or those persons.

513 In the present case, there is no direct evidence of the formation of an agreement. That situation is not uncommon; conspirators commonly act in secret. A conspiratorial agreement often has to be inferred from other evidence, particularly evidence about the conduct of the alleged conspirators. Counsel for the applicants submitted that, when Sharman acquired the Kazaa business from Kazaa BV, its principals knew that the operation of the Kazaa system had caused, and would continue to cause, damage to sound recording companies, including the first to sixth and eighteenth applicants. Yet the people concerned with the management of Sharman determined to operate the business. It is said those concerned with the management of Altnet, having the same knowledge, joined them in doing so.

514 I do not doubt that, at all material times, those concerned with the management of Sharman and Altnet realised that the operation of the Kazaa system routinely caused significant loss to sound recording companies, including the first to sixth and eighteenth applicants. I also do not doubt such losses have been sustained. However, this is not sufficient. In *McKernan v Fraser* (1931) 46 CLR 343 at 362, Dixon J said it was 'settled that, for a combination or acts done in furtherance of the combination to be actionable in such circumstances, the parties to the alleged conspiracy must have been impelled to combine, and to act in pursuance of the combination, by a desire to harm the plaintiff, and that this must have been the sole, the true, or the dominating, or main purpose of the conspiracy'. That cannot be said in the present case. Those of the respondents who were involved in making the agreements relating to Kazaa were almost certainly unconcerned about the adverse effect of those agreements on the applicants, but that effect was neither the sole nor main purpose of the agreements. The dominant purpose of the agreements was to make money.

515 Conspiracy by unlawful means includes the element that the conspirators agreed to carry out their objectives by unlawful means. It may be assumed, for present purposes, that those respondents who participated in the Kazaa agreements realised, and at least tacitly agreed, that implementation of their agreements would involve them in authorising infringements of copyrights and, therefore, acting unlawfully. However, that is not sufficient. It is true that, where the conspiracy involves unlawful means, it is not essential that its purpose be solely or mainly to injure the plaintiff. However, this must be at least one of the purposes of the conspiracy: see *McWilliam v Penthouse Publications Ltd* [2001] NSWCA 237 at [12] and *Dresna Pty Ltd v Misu Nominees Pty Ltd* [2004] FCAFC 169; [2004] ATPR 42-013 at [7]. The evidence in the present case does not establish such a purpose. It is not enough that the conspirators were indifferent to the effect of their actions on the plaintiff.

516 Neither of the argued bases of the tort of conspiracy has been established. That part of the applicants' claim fails.

VIII DISPOSITION

517 The applicants' copyright claim succeeds against six respondents: Sharman, LEF, Ms Hemming, Altnet,

BDE and Mr Bermeister. I propose to make two declarations concerning those respondents. One declaration will state that the six respondents have infringed the copyright in each of the Defined Recordings by, first, authorising Kazaa users to make a copy of the said recording and to communicate the recording to the public, in each case without the licence of the relevant applicant; and, second, by entering into a common design to carry out, procure or direct that authorisation. The other declaration will be that the six respondents threaten to infringe the copyright of the applicants in other sound recordings in the same way.

518 On several occasions, before and during the trial, I emphasised that this trial was the occasion for the parties to put forward any evidence they thought to be relevant to the nature and form of relief, other than pecuniary relief. However, I mentioned the possibility of allowing the parties an opportunity to make submissions in relation to the form of any injunctive relief.

519 I have formed some views about the appropriate form of injunctive relief and have drafted some orders. It is convenient immediately to make the orders. However, I will do so on a provisional basis, in the sense that I will be prepared to reconsider the form of the orders, if so requested by any party. I will not receive further evidence in relation to the nature and form of the orders.

520 Subject to that comment, I think it is appropriate to grant an injunction to restrain future infringements of the applicants' copyrights. This injunction should be couched in general terms, reflecting the relevant respondents' general obligation not further to infringe the applicants' copyright. However, I am 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. There needs to be an opportunity for the relevant respondents to modify the Kazaa system in a targeted way, so as to protect the applicants' copyright interests (as far as possible) but without unnecessarily intruding on others' freedom of speech and communication. The evidence about keyword filtering and gold file flood filtering, indicates how this might be done. It should be provided that the injunctive order will be satisfied if the respondents take either of these steps. The steps, in my judgment, are available to the respondents and likely significantly, though perhaps not totally, to protect the applicants' copyrights.

521 Accordingly, I propose to make an order restraining the six infringing respondents from further infringing the applicants' copyright in any sound recordings by authorising the doing in Australia by Kazaa users of any infringing acts, in relation to any sound recording, the copyright of which is held by any of the applicants, without the licence of the relevant copyright owner.

522 There will be orders providing, in effect, that continuation of the Kazaa Internet file-sharing system will not be regarded as a contravention of the general injunctive order if the system is first modified, in a manner agreed by the applicants or approved by the Court, to ensure keyword filtering or gold file flood filtering. To allow this to happen, the operation of the injunction will be stayed for two months.

523 The copyright claims will be dismissed as against Sharman Holdings, Mr Morle, BDE Pty Ltd and Mr Rose.

524 The TP Act and conspiracy claims will be dismissed as against all respondents.

525 Costs orders will be made in favour of the parties who have succeeded in relation to the copyright claims. However, in recognition of the fact that the costs incurred by the infringing respondents have been increased by the applicants' inclusion of unmeritorious TP Act and conspiracy claims, the costs payable to the applicants by those respondents will be reduced by 10%.

526 One or more of the parties may wish to appeal against aspects of my orders. As the orders do not provide final relief in the proceeding, leave to appeal would be necessary. It may be helpful if I indicate I would be disposed to grant leave to appeal, on application for that purpose, subject to two conditions: first, that the applicant for leave undertakes to prosecute the appeal diligently and with a view to obtaining a hearing in the February 2006 Full Court sittings; and, second, that, during the pendency of the appeal, the parties discuss, and endeavour to agree, the terms of the protocol referred to in order 5.

I certify that the preceding five hundred and twenty-six (526) numbered paragraphs are a true copy of the Reasons for Judgment herein of the Honourable Justice Wilcox.

Associate:

Dated: 5 September 2005

Counsel for the Applicants:	Mr A J L Bannon SC, Mr J V Nicholas SC, Mr R Cobden, Mr J M Hennessy, Mr C Dimitriadis, Mr S W Balafoutis
Solicitors for the Applicants:	Gilbert + Tobin
Counsel for the First to Fourth Respondents:	Mr A J Meagher SC, Mr N R Murray
Solicitors for the First to Fourth Respondents:	Clayton Utz
Counsel for the Fifth Respondent:	Mr R J Webb SC
Solicitors for the Fifth Respondent:	Ebsworth & Ebsworth
Counsel for the Sixth to Ninth Respondents:	Mr S G Finch SC, Mr M J Leeming

Solicitors for the Sixth to Ninth Respondents:	Landerer & Co
Counsel for the Tenth Respondent:	Mr B W Walker SC, Mr K M Connor
Solicitors for the Tenth Respondent:	Ebsworth & Ebsworth
Counsel for the Amici Curiae (Australian Consumers Association Pty Ltd, Electronic Frontiers Australia Inc and New South Wales Council for Civil Liberties Inc):	Mr G McGowan SC, Ms L De Ferrari
Solicitors for the Amici Curiae (Australian Consumers Association Pty Ltd, Electronic Frontiers Australia Inc and New South Wales Council for Civil Liberties Inc):	Communications Law Centre
Dates of Hearing:	29, 30 November 2004 1, 2, 3, 7, 8, 9, 10, 11, 15, 16, 17 December 2004 17, 31 January, 2005 22, 23 March 2005
Date of Judgment:	5 September 2005