Extended case note and commentary*: Sony Music Entertainment (Australia) Limited & others v. University of Tasmania & others [2003] FCA 532 (30 May 2003)

Dr Adrian McCullagh and Professor William Caelli

Dr. Adrian McCullagh is a solicitor at Freehills and Adjunct Professor in Electronic Commerce Law at the Information Security Research Centre at the Queensland University of Technology. Professor William Caelli is Head of the School of Software Engineering and Data Communications at the Queensland University of Technology

Background

This case involves the legal rights of a copyright holder to seek discovery using computer forensic tools which may (in fact usually do) cover many records stored on a computer that are not relevant to the issues at hand.

Even though this case only concerns an interlocutory application it is a case that should be watched as it involves peer to peer networks and possible infringement of copyright of sound recording in digital music. Further, it is the first case of its kind to be heard by an Australian court and exhibits the recording industry's new approach of proceeding against individuals as opposed to the producers of the tools that can be used to distribute copyright infringing material[1].

Facts

Sony Music is the copyright owner or exclusive licensee of a substantial number of sound recordings and it is very concerned about the proliferation of MP3 and other formatted digital music files that are distributed via "peer to peer" networks. In order to understand the implications of this case it is an advantage to have some understanding of the technology involved.

(a) What is MP3[2]

MP3 is, in simple terms, a compression algorithm that will reduce the length of large files into more manageable sizes without, or minimally, reducing the quality of the information it represents. MP3 has become very popular for the compression of sound recording and audio-visual material. These files are, in normal mode, generally very large and quite cumbersome to transfer over the internet. Without compression technology it would be uneconomic for sound files and audio-visual/video files to be transferred over the internet as they would need a high bandwidth for reasonable transmission times. Systems with restricted bandwidth require more time for transfers to be effected. That is, from a file transfer perspective it is much faster to transfer files over the internet when the user has a high bandwidth facility like ADSL[3] than it is when using a 56k modem facility. In the past most users were restricted to 56 Kbs[4] (kilo bits per second), or less, modem transfers. Broadband is generally regarded in Australia as having a minimum of 2 Mbs (mega bits per second) file transfer capability. That is, the minimum broadband capability is 40 times faster that modem transfers. In many other jurisdictions, a file transfer is regarded as being "broadband" when the file transfer capability is at a minimum of 8 Mbs.

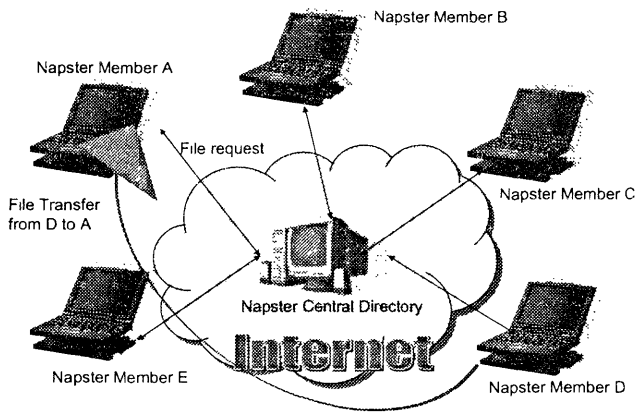
MP3 was developed by the Motion Picture Expert Group (MPEG) number 3 (hence the name MP3, itself a shortened form of the term "MPEG audio layer 3") as an international compression standard for sound recordings and audio-visual material. By compressing the size of the file less bandwidth would be needed. Some files like audio-visual files could be 100 mega bits in size or more. So any transfer of this file over a non-broadband mechanism could take up to 29.76 minutes and this is if the connection remains intact. With broadband capability the same transfer could take between 12 to 50 seconds.

(b) What is a Peer to Peer (P2P) Network

A "peer-to-peer" network is regarded as one in which each node of the network appears on equal footing with any other member node of the network. No recourse is required, for information flow, etc. to a centralised directory of files, services, nodes or the like. The term should be contrasted with other terms such as "client-server" networks and the like. Technically speaking the Napster facility was not a pure peer to peer network as the ability to locate a particular sound recording was controlled in part by a central directory operated by Napster Inc.

The Napster network, arguably the most famous music/video sharing network was structured as follows:

Napster structure for "File Sharing"



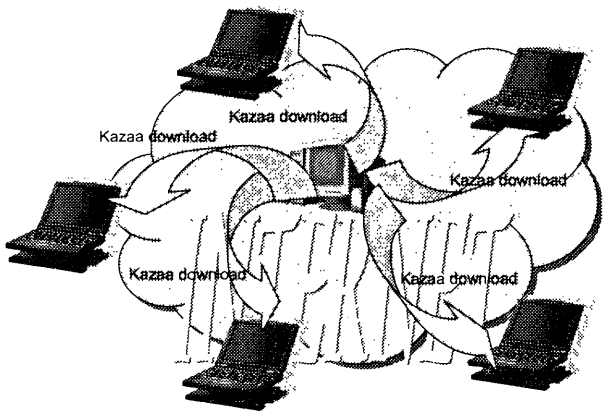
The Napster network involved the listing by members of MP3 or other files (sound recordings) together with an IP address or URL locator. The actual MP3 files would remain stored on each member's computer in a shared directory. The listing was stored on a central database that was under the control of Napster Inc. If a member wanted a particular song he/she would search the data base (make a request) and if there was a match he/she would then contact the member holding the copy of the wanted sound recording. Once contact was made the members would exchange details and the sound recording would be transferred.

It was held by a US district court that the system was illegal as Napster was committing contributory infringement of copyright.

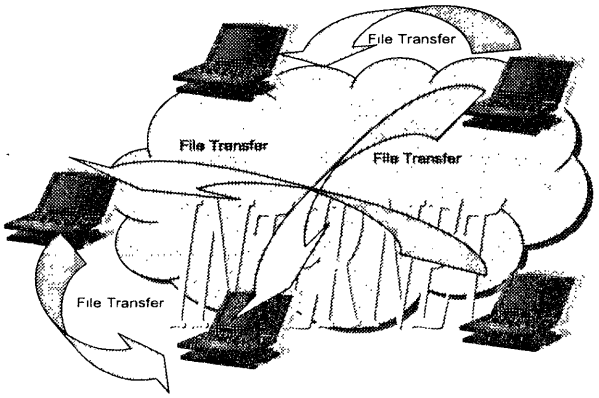
After Napster, other P2P systems have come to fruition. The most notable today are Morpheas[5] and Kazaa[6]. Both these systems have been subject to extensive litigation but have not fallen foul of the Court system. Recently a Californian Court[7] held that Morpheas and Kazaa were capable of multiple uses which included legitimate and non legitimate applications. The defendant in that case was able to argue successfully in the same manner as the *Sony v. Paramount Pictures*[8] case regarding VCR's that since there was a legitimate use which was not insubstantial that the publishers of both Morpheas and Kazaa were not liable for contributory infringement of copyright material[9].

Morpheas and Kazaa create a shared directory mechanism and associated maintenance protocol between users. There is no centralised membership facility but people download from the Kazaa site the Kazaa program. The Kazaa program will create a shared file directory on the down loader's system, which will permit other people who have the Kazaa program to gain access to that shared file directory, provided such sharing capability has been granted. This directory may or may not contain copyright infringing material.

Therefore the first step is for the user to download a copy of the Kazaa software as follows:



Once the download is complete each end user is in a position to transfer files with other Kazaa end users as follows:



The difficulty is to locate other users who have the Kazaa software and have granted shared directory capability. Since there is no central directory, which was the down fall for Napster, it is difficult for the copyright holders to cost effectively identify who has infringing copyright material on their computer systems. It is for this reason that the major copyright holders, namely the major players in the music industry and the motion picture industry, are now approaching universities as a source of information to identify who may possess infringing copyrighted material.

It is important to note that Kazaa and like systems "synchronise" the shared directory between willing users of the system[10]. In other words, if two people start using Kazaa they will each hold a copy of a "sharing" directory that Kazaa will syn-chronise between them. Thus, if one person adds some new file entries to the directory, the Kazaa protocol will ensure that the other party's copy of the "sharing" file directory is synchronised (updated). Now, as each person introduces a new person to, say, a group, the sharing directory of each system is synchronised between all in that group. In this way, a Kazaa directory will automatically "grow" as new "shared file" entries are made by cooperating users. The important aspect of the Kazaa system is that members are not required to communicate with the Kazaa central system in order to effect the file transfer. That is, effectively the Kazaa system is not involved in the transfer protocol.

Issues

(a) Forensic Issue

Forensic IT soft-ware tools such as "Encase"[11] cannot easily distinguish between computer records that are subject to discovery and those which are not. Although it is possible to operate Encase in manner that is non-invasive through the preview capability which is expressly designed for the purpose of determining whether a system contains evidence within the scope of an investigation before imaging any of the material located on the relevant secondary memory. Encase is a software program that will take a compressed bit-image copy of the hard drive and any other secondary memory locations on a computer.

Encase takes this bit-image copy of a hard drive's contents in such a way as not to disturb any of the file meta-information located on the hard drive. This in effect preserves all file access

times and, according to the documentation provided by owners of Encase, the compression algorithm used by Encase does not lose any of the original information. Hence Encase does not take a one to one correspondence copy of what is on the target machine but instead creates a compressed copy of the information stored on the target machine. The owners of Encase state that the compressed copy can be reconstituted to exactly what was on the target without loss of any information. This, as far as the authors are aware, has yet to be challenged or established by any Court in Australia[12]. In addition, Encase appears to not have been evaluated under internationally recognised standards such as IS15408, the so-called "Common Criteria".

Encase takes a read only copy of the target computer's hard drive. Being read only, the forensic copy can be preserved without corruption[13]. Other forensic systems use an alternative procedure. These systems will immediately after the first compressed bit-image-copy (copy-1) has been taken, copy the copy-1 so as to preserve the evidence that has been gathered and generate copy-2. This does not as far as the author is aware occur with Encase. It is copy-2 that is analysed by the investigator. The reason for this is that in many cases the target computer will be in an active state and will need to continue with other processes. In effect copy-1 is a copy state of a computer as at a particular point in time. In many cases the copy-1 is time stamped. Copy-2 is a working copy of copy-1, which is sometimes known as the "analysis copy". If for any reason copy-2 is damaged or corrupted, a further copy of copy-1 is taken which will be used as the analysis copy.

Sony Music wanted to use Encase to identify whether the University of Tasmania's computer system held any unauthorised copies of sound recordings and in whose name the sound recordings were so held. The University's computer system was partitioned into user accounts and if a sound recording were located on the University's system the relevant partition would identify the particular user's account. It was the user accounts which held unauthorised sound recordings that Sony Music was after by way of evidence.

(b) Legal Issues

Sony Music sought preliminary discovery pursuant to O15A rr. 3,6,12 of the Federal Court Rules. The Universities had opposed the application on the basis that it was beyond the Court's power to grant such an order regarding documents which go beyond the language of the rules. That is, the order sought for preliminary discovery by Sony Music would include many documents that would not be relevant to the particular case and as such were not within the terms of the Federal Court Rules. Further, the Universities were concerned about breaches of privacy regarding student information stored on their respective computer systems.

Rule 3 concerns preliminary non-party discovery whereas rule 6 concerns preliminary party discovery. That is, rule 3 provides in part that:

> *where an applicant (Sony) having made reasonable enquiries, is unable to ascertain the description of a person (the University Students) sufficiently for the purpose of commencing a proceeding in the court against that person (the person concerned) and it appears that some person (the Universities) has or are likely to have knowledge of facts ... or is likely to have had possession of any document ... tending to assist in such ascertainment, the court may make an order under sub-rule (2)...*
>
> *(2) The court may order that the person (the Universities)... , shall:*
>
> *...(b)make discovery to the applicant (Sony) of all documents which are or have been in the person's or its (the Universities') possession relating to the description of the person concerned (the University Students).*

Rule 6 concerns an application for an order for preliminary discovery against a prospective respondent. It is difficult to understand why Sony made an application against the Universities under this rule as it appears that Sony was never intending to commence proceedings against the Universities but was simply seeking preliminary discovery against the Universities to ascertain the names of University Students who allegedly were contravening Sony's copyright through the transmission of MP3 files.

Arguments

(a) Sony & others

Sony had engaged Mr Thackray who was an IT forensic expert. A substantial aspect of Sony's argument was that the search methodology proposed by the University was inadequate and therefore Sony wanted to use IT forensic technology to identify which students (if any) had in the respective student account directory infringing copyright material.

Sony acknowledged that the material extracted through the IT forensic mechanism would extract much more information than would be relevant for the purpose of the discovery. According to Sony and in evidence by Thackray it was impossible during the extraction process to determine what information was relevant for the anticipated litigation. This determination could only be undertaken after the extraction process was complete and this was a separate exercise involving the analysis of each record to determine its relevance. Sony was willing to give certain undertakings in favour of the court so as to protect any parties who were not directly subject to the discovery process.

(b) University of Tasmania & others

The Universities argued that:

(a) much of the material that would be extracted/copied from the University computers would be irrelevant material and the exercise was really a fishing expedition;

(b) the Universities were subject to privacy obligations and therefore the extraction would not be legal and could jeopardise the

Universities' and its students' rights;

(c) the Universities instead of permitting a bitmap copy of their system to be undertaken proposed a copy of a limited number of files that had the suffix of either ".mp3" or ".wma". That is, the Universities would deliver on a confidential and privileged basis a file containing each file located having:

(1) "mp3", "wma", "rm", "ogg", or "zip" extensions;

(2) "jpeg", "bmp", "tiff" "gif", "psd" or "emf" extensions;

(3) containing one or more of the following words:

(A) "ripping", "rip", "rips" or "ripper";

(B) "music", "recording", "record", "song" or "sound file";

(C) "download", "downloading", "upload", "uploading", "uploaded", "post" or "posting";

(D) "mp3", "wma", "rm", "ogg" or "zip";

(E) "jpeg", "bmp", "tiff", "gif", "psd" or "emf"; or

(F) "CD", "CDs", "CD-/R", "CD-/W", "CD-/RW", "tape" or "mini-disc".

Judicial Analysis (Tamberlin J. Federal Court)

The Court noted that central to the dispute was the level of particularity at which the expression "document" should be applied to records stored on CD ROMs, and computer hard drives.

Each of the Universities had called their respective "Computer System Officers" to give evidence of the methodology that they would each implement to extract discoverable material from the computer hard drive. There was not much difference in the methodologies proposed by each of the experts called by the Universities. The Court noted that according to the evidence of Thackray, the search methods proposed by the Universities were inadequate to properly investigate the suspected infringements. The Court accepted that Thackray was providing a superior methodology that was more complete than that proposed by the Universities. A further point was that the University methodology would only identify those files that were still in existence and would not pick-up deleted files. The forensic methodology would also identify deleted files and may be capable of re-establishing them. This would provide evidence of past infringing copies if they existed.

The Court noted the Court's discretionary powers in granting the orders sought by both parties and sided with Sony in this case provided certain protective measures were given as undertakings. In particular, the court stated:

> *"I am satisfied that if the narrow search tools and methods proposed by the Universities ... are used, then it is likely that there will be insufficient discovery".*

Further, the Court in giving its decision stated:

> *"Another matter to be weighed in balancing factors in the exercise of discretion is the public interest in having full and proper disclosure by way of preliminary discovery in order to ensure that an informed decision can be made as to whether to commence proceedings and against whom they should be brought"* (emphasis added).

This appears to have been the crux of the Court's thinking as it was possible to deal with the privacy issue by way of appropriate undertaking being given but it was not possible to deal with the failure to reach a proper disclosure without giving the orders being sought by Sony.

Commentary

This is an important case as it follows the same position that is occurring in other jurisdictions regarding the gathering of evidence located on computers. Further it is an acknowledgement as to the possible forensic benefit of packages like "Encase". But it appears that there was little argument as to how the "Encase" program works and whether it is accurate in its evidence gathering capability. Nor was there any argument as to issues of integrity of any evidence being gathered. These issues may arise in other aspects of this case as and when they occur.

It is unfortunate that the court did not delve into the issue of actual identification of what files comprise sound recording files versus those that do not. For example, there is nothing to stop any user labelling a file with the extension name ".MP3" which could stand for any personal term, e.g. "My program number 3", nor such a file being labelled with the user's name that may correspond to a prominent entertainer, e.g. a file named "stewart.mp3" could be compressed data from a Ms Stewart's doctoral research activity compressed using the mp3 scheme rather than a copy of a sound recording by "Rod Stewart", a popular performer. Moreover, legitimate compressed sound files that utilise the "mp3" compression scheme may exist in storage, e.g. recordings of voices from psychology experiments, sound recordings of audio transformed signals from radio astronomy data, and of course the list could go on. It is normal for investigatory programs to actually attempt to read the actual content of files in directories and try to "pattern match" to determine if a sound file is present, irrespective of the name given to such a file. This may mean that the contents of such files may be subject to full exposure. In addition, even if a sound file is identified this does not mean that it is an illegitimate file. In opposition, there is nothing to stop an illicit copy of a digital sound recording being labelled in a completely proprietary way.

A further point about this case is that the court has in effect condoned an organisation, in this case Sony, to undertake a fishing expedition for evidence in the possession, power or control of a third party. It is similar to an order that party A (Sony) has the right to rifle through a filing cabinet or filing cabinets under the possession power or control of party B (the Universities) so as to locate some information (the certainty of which is unknown) that may incriminate party C who at the time is indeterminate (unknown university students). Traditionally this has not been

condoned at common law but as was noted by Burchett J, in *Paxus Services Ltd. V. People Bank Pty Ltd*[14]:

> *"It is no answer to the applicant's application under rule 6 to say that the proceeding is in the nature of a fishing expedition. ... Rule 6 is designed to enable an applicant, in a situation where his proof can rise no higher than the level the rule describes, to ascertain whether he has a case against the prospective respondent, that is to "fish" in the old cases".*

It appears that the fishing expedition argument is equally inappropriate for rule 3 as it is for rule 6. Tamberlain J. has, by granting the order sought by Sony, permitted Thackray to implement a fishing expedition on the documents and records stored on the Universities' computer systems. Sony through Thackray's evidence challenged successfully the evidence gathering methodology that was going to be deployed by the Universities and therefore, subject to certain undertakings given to the Court, is able to gather substantially more information than what was really needed for the purposes of Sony's case.

It appears that there is a growing trend by the courts to make expansive orders when the matter involves computer records. This position may soon be clarified as currently there is before the High Court the case of *TLC Consulting v. White*[15] which case concerns whether a "computer server" can be classified as a record or whether it is a medium that contains many records some of which may not be relevant to the proceeding at hand.

In the United States mistakes concerning alleged copyright infringement have happened. The Recording Industry Association of America (RIAA) recently sent a formal apology to Penn State University due to an incorrect notice of alleged Internet copyright infringements. It appears that RIAA had used a software tools to identify allegedly infringing material located on the Penn State computer system within the Department of Astronomy and Astrophysics but instead the software had mis-identified the material[16].

An issue that has yet to be determined is whether the evidence gathered by Thakray will be admissible. Notwithstanding its admissibility, it is still within the courts' discretion to completely discount such evidence. Recently, a Higher Regional Court of Düsseldorf held that log files produced by software tools that measured and recorded internet traffic were immature as evidence gathering mechanisms and therefore could not be taken as prima facie evidence of the correctness of the information so gathered[17]. That is, the court required further proof that the evidence presented as a result of these software tools operated in a correct manner so as to produce valid evidence.

Only time will tell whether forensic IT evidence will be acceptable to the courts. But the Sony case is the first step in what may be a long and perhaps bumpy road to the acceptance of forensic IT evidence. Unfortunately IT forensic evidence is no where near as exciting as CSI[18].

---

* The authors would like to thank Professor George Mohay, of the Faculty of Information Technology at the Queensland University of Technology who provided guidance regarding "Encase", and Mr. Michael Fernon a Partner at Freehills. Both were kind enough read this paper and provide some very pertinent suggestions. Any remaining errors of course lay with the authors.

1 On 23 April 2003, the Recording Industry Association of America commenced copyright infringement proceedings against 1 Princeton University student, 2 Rennselaer Polytechnic Institute students and 1 Michigan Technology University student. Atlantic Recording Corp,. et al. v. Peng Atlantic Recording Corp,. et al v. Jordan Atlantic Recording Corp,. et al. v. Sherman Atlantic Recording Corp,. et al v. Nievlt See http://news.findlaw.com/legalnews/docu ments (accessed 2 July 2003)

2 MPEG -audio layer 3 as developed by the Motion Picture Expert Group http://www.mpeg.org/MPEG/mp3.html (accessed on 2 July 2003)

3 Asynchronous Digital Subscriber Line

4 The actual transmission throughput of a 56 Kbs modem is usually substantially less than 56 Kbs. Usually, the throughput varies between 14 Kbs to 36 Kbs depending of many factors that are not relevant to this discussion. Rarely, does a 56 Kbs modem operate above 36 Kbs.

5 http://www.morpheus.com/ (accessed 2 July 2003)

6 http://www.kazaa.com/us/index.htm (accessed 2 July 2003)

7 Metro Goldwyn Meyer Studios et al v. Grokster Ltd. Et al http://www.eff.org/IP/P2P/MGM_v_Grokster/030425_order_on_motions.pdf (accessed 2 July 2003)

8 Sony Corp. v. Universal City Studios Inc. 464 U.S. 417 (1984) http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=US&vol=464&invol=417 (accessed 2 July 2003)

9 The issue of "contributory infringement" is dealt with by the Australian Courts under the guise of direct and indirect authorisation to infringement. See University of New South Wales v. Moorehouse (1975) 133 CLR 1

10 Good, N., and Krekelberg, A., "Usability and Privacy : a study of Kazaa P2P file Sharing"http://www.hpl.hp.com/shl/papers/kazaa/KazaaUsability.pdf (accessed 2 July 2003)

11 "Encase" is a software program developed by Guidance Software Inc. http://www.guidancesoftware.com/ (accessed 2 July 2003)

12 The owners of Encase in their documentation entitled "Encase legal journal" at page 52 make reference to the case of State v. Cook 777 NE 2d 882 (Ohio Appeals 2002) where the court in that case did endorse the evidence gathered via Encase as being the best evidence available. See also People v. Rodriguez: Somona County, California Superior Court, no. SCR28424

13 There is a risk with this procedure. Since there is only ever one copy of the target systems files in existence (a read only copy "copy-1"), if the copy-1 for whatever reason was corrupted then it would be necessary for another copy be taken from the target system. But this may be useless as the target system could have been used since the first copy was taken and thus vital evidence could have been lost or destroyed in the time lapse.

14 (1990) 99 ALR 728 at 733

15 see TLC Consulting Services Pty Ltd v. White [2003] QCA 131, where the Queensland Court of Appeal has recently determined that a "server" falls within the ambit of the definition of "record". It had been argued that the Queensland Office of Fair Trading was exceeding its powers when it confiscated TLC's computer server as opposed to taking a copy of the hard drive or parts of the hard drive that contained the relevant evidence. On 25 June 2003, leave to appeal was granted by the High Court to TLC Consulting Pty Ltd. See http://www.austlii.edu.au/au/other/hca/transcript/2003/B14/5.html

16 "RIAA apologises for threatening letter" http://www.zdnet.com.au/newstech/security/story/0,2000048600,20274439,00.htm

17 OLG Duesseldorf, Decision of February 26, 2003 The authors would like to thank *Christoph Rittweger* and *Isabelle Bulenda* of the Munich office of Baker and Mackenzie Lawyers

18 Crime Scene Investigation. A television program produced in the US as seen on Channel Nine.