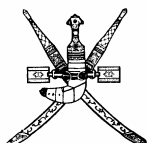


WIPO/IPR/MCT/03/1

ORIGINAL: English

DATE: November 28, 2003



SULTANATE OF OMAN



WORLD INTELLECTUAL
PROPERTY ORGANIZATION

WIPO NATIONAL SEMINAR ON ENFORCEMENT OF INTELLECTUAL PROPERTY RIGHTS FOR GENERAL PROSECUTORS

organized by
the World Intellectual Property Organization (WIPO)

in cooperation with
the Ministry of Commerce and Industry

Muscat, December 1 and 2, 2003

COPYRIGHT INFRINGEMENT : CASE STUDIES

*Lecture prepared by Dr. Uma Suthersanen, Senior Lecturer and Senior Fellow,
Queen Mary Intellectual Property Research Institute/Centre for
Commercial Law Studies, University of London*

CASE 1 - RIAA v. THE RIO PLAYER

*Recording Indus. Association of America, Inc. v. Diamond Multimedia Systems Inc.*¹ represents the first major case concerning the MP3 technology whereby the recording industry decided to test the ambit of the Audio Home Recording Act (AHRA).² The case's discussion on the applicability of AHRA is pertinent: the main thrust of AHRA is to ensure that there is payment of levies upon the sale or distribution of digital audio recording devices. This "blank levy" system ensures that some monies are collected from the use of audio devices, which are subsequently distributed to interested copyright parties. The second portion of AHRA fulfils the "rights management" requirement within the WIPO Treaties: AHRA requires the use of copy control systems in digital audio recording devices, specifically the Serial Copyright Management System (SCMS).³ The final interest in the case is the *obiter* remark of the court in relation to space-shifting activities, a remark relied upon by Napster in defending its own activities.

The Rio Technology

The defendant, Diamond, was the manufacturer of a portable, hand-held playing device (the Rio player), which was capable of receiving, storing, and re-playing MP3 files: these files were transferred to the Rio player from the hard drive of a personal computer. The appeal of the Rio player was that it allowed a user to download MP3 audio files from a computer and to listen to them elsewhere. It should be noted that the Rio player cannot effect any transfer of MP3 files; instead, users must use the Rio Manager computer software provided to download the MP3 file from a computer's hard drive to the Rio itself via a parallel port cable that plugs the Rio into the computer. Furthermore, the Rio device is incapable of receiving MP3 files from anything other than a personal computer equipped with Rio Manager. The Rio device is solely aimed at playing music: it cannot make duplicates of any digital audio file it stores, nor can it transfer or upload such files to a computer, to another device, or to the Internet. Users can, however, purchase additional flash memory cards to which MP3 files can be downloaded on to; these cards can then removed from one Rio and played back in another.⁴

Audio Home Recording Act (AHRA)

The statute does not prohibit the copying or transmission of copyright works in audio recordings as such: it merely places a duty on manufacturers to place the industry-wide copyright management system on to recording devices. Thus, the act states that

"[n]o person shall import, manufacture, or distribute any digital audio recording

¹ 29 F.Supp.2d 624 (C.D.Cal.1998), 180 F.3d 1072 (9th Cir. 1999).

² The Audio Home Recording Act 1992, codified as Chapter 10, U.S. Copyright Act.

³ RIAA also sought payment of royalties under §1003, AHRA, as owed by Diamond as the manufacturer and distributor of a digital audio recording device.

⁴ At the time of the trial, the Rio could store approximately one hour of music or sixteen hours of spoken material: however, technological capabilities have expanded and current portable MP3 players can store up to 600-1000 hours of music.

device ... that does not conform to the Serial Copy Management System ["SCMS"] [or] a system that has the same functional characteristics."⁵

The first issue was whether the Rio player was a "digital audio recording device". This, in turn, is defined by the Act as follows:

"any machine or device of a type commonly distributed to individuals for use by individuals, whether or not included with or as part of some other machine or device, the digital recording function of which is designed or marketed for the primary purpose of, and that is capable of, making a *digital audio copied recording* for private use...."⁶

A "digital audio copied recording" is defined as:

"a reproduction in a digital recording format of a digital musical recording, whether that reproduction is made directly from another digital musical recording or indirectly from a transmission."⁷

First, does the Rio player record directly from another digital musical recording? At some point of the transfer of an MP3 recording to the Rio player, the file must pass through the hard drive of a computer: in this case, the question then is whether the hard drive of a computer is a digital music recording? The court reasoned that

"...computers (and their hard drives) are not digital audio recording devices because their "primary purpose" is not to make digital audio copied recordings. Unlike digital audio tape machines, for example, whose primary purpose is to make digital audio copied recordings, the primary purpose of a computer is to run various programs and to record the data necessary to run those programs and perform various tasks...The legislative history thus expressly recognizes that computers (and other devices) have recording functions capable of recording digital musical recordings, and thus implicate the home taping and piracy concerns to which the Act is responsive. Nonetheless, the legislative history is consistent with the Act's plain language--computers are *not* digital audio recording devices."⁸

Does this mean that if an MP3 file is transmitted intermittently through a computer before reaching a playing or recording device, such devices need not be covered by the copyright management system (nor indeed, be subject to the AHRA levy system)? The court's answer is affirmative:

"Thus, the Act seems designed to allow files to be "laundered" by passage through a computer, because even a device with SCMS would be able to download MP3 files lacking SCMS codes from a computer hard drive, for the simple reason that there would be no codes to prevent the copying."⁹

⁵ 17 U.S.C. § 1002(a)(1), (2).

⁶ *Ibid.*, §1001(3).

⁷ *Ibid.*, §1001(5)(b).

⁸ *Ibid.*, at p. 1078.

⁹ *Ibid.* at p. 1079.

Thus, in respect of the first definitional aspect, the 9th Circuit was of the opinion that the Rio Player could not be said to record directly from "digital music recordings": it recorded directly from the hard drive of a computer, and a hard drive is excluded from the definition of digital music recordings.

Could the Rio player be held to reproduce digital music recordings from transmissions, which is the second basis under AHRA for imposing copy management systems on devices? RIAA asserted that indirect reproduction of a transmission is sufficient for the Rio to fall within the Act's ambit as a digital audio recording device. However, since the Rio player only directly reproduces files from a computer hard drive via a cable linking the two devices (this was held "obviously" not to be a transmission), it can only be said to indirectly reproduce a transmission. Did indirect reproduction of a transmission fall within the statutory definition?

The court answered in the negative. In effect, the court held that the most logical reading of the Act was that a device could be said to fall within the Act's provisions if it was able to indirectly copy a digital music recording by making a copy from a transmission of that recording. However, Rio's technology prevented this: the player cannot make copies from transmissions, but instead, can only make copies from a computer hard drive. Furthermore, any transmission reproduced indirectly must pass through a computer to reach the Rio.¹⁰ In other words, it appears that if a computer is involved at any stage of the reproduction or transmission activity of a technical device, AHRA cannot apply. The downside of this decision was subsequently felt in the *Napster* decision: the non-application of AHRA includes the non-application of its defences, especially in relation to non-commercial use by consumers (discussed below).

Space Shifting is Non-commercial Personal Use

A further impact of this decision arose from an *obiter* comment by the court. It stated that, in any event, Rio's operation was entirely consistent with the AHRA's main purpose - the facilitation of personal use. The Rio merely makes copies in order to render portable, or "space-shift," those files that already reside on a user's hard drive:

Such copying is paradigmatic noncommercial personal use entirely consistent with the purposes of the Act.¹¹

On a more general perspective, at this stage of technological developments, the 9th Circuit, unlike in the *Napster* case, was unconvinced as to whether Internet piracy causes harm to the plaintiff's market. As part of its general claim, RIAA asserted that Internet distribution of serial digital copies of pirated copyrighted material would discourage the purchase of legitimate recordings, predicting that losses to digital Internet piracy would soon surpass the \$300 million that is allegedly lost annually to other more traditional forms of piracy. However, the court countered this allegation with a study which stated that a willingness to download illicit files for free does not correlate to lost sales as persons willing to accept an item for free often will not purchase the same item, even if no longer freely available; furthermore, the current price of commercially available recordings offsets, in part, the losses

¹⁰ *Ibid.* at pp. 1080-1082.

¹¹ *Ibid.* at p. 1079.

incurred by the industry from home taping and piracy.¹² Interestingly, the support of the 9th Circuit for this argument was not to continue.

CASE 2: RIAA v. MP3.COM

The second major decision is *UMG Recordings, Inc. v. MP3.com, Inc.*¹³, where the District Court found that reproduction of audio CDs into MP3 format did not "transform" the work; furthermore, the court found that space-shifting of MP3 files was not a fair use. The recording industry sued MP3.com when it launched its "My.MP3.com" service. The advertising promised subscribers that they could store, customize and listen to the recordings contained on their CDs from any place where they have an Internet connection. In order to fulfil subscriber demands, the defendant purchased tens of thousands of popular CDs in which plaintiffs held the copyrights, and, without authorisation, copied their recordings onto its computer servers so as to be able to replay the recordings for its subscribers.

It should be noted that the recordings were not available to all users: in order to access a recording, the MP3.com subscriber had to "prove" that she already owned the CD version of the recording by inserting her copy of the commercial CD into her computer CD-Rom drive for a few seconds. The alternative means of accessing the recordings on the site was to purchase the CD from one of defendant's co-operating online retailers. Only by these two means could the subscriber access, via the Internet from a computer anywhere in the world, the copy of plaintiffs' recording made by defendant. The defendant relied on the argument that such copying is protected under the "fair use" defence, and specifically on the space-shifting activity. However, the court held:

Although the defendant seeks to portray its service as the "functional equivalent" of storing its subscribers' CDs, in actuality the defendant is re-playing for the subscribers converted versions of the recordings it copied, without authorization, from plaintiffs' copyrighted CDs."¹⁴

The U.S. copyright law calls for the analysis of four factors in determining whether the fair use defence applies:

- a) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;
- b) the nature of the copyrighted work;
- c) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and
- d) the effect of the use upon the potential market for or value of the copyrighted work.¹⁵

¹² *RIAA v. Diamond Multimedia Systems Inc.*, 180 F.3d 1072 (9th Cir. 1999), at p. 1074.

¹³ 92 F. Supp. 2d 349 (S.D.N.Y., 2000).

¹⁴ *Ibid.*, at p. 350.

¹⁵ 17 USC §107.

The court worked its way quickly through the defendants' argument, rejecting all of them. In relation to the first factor, the defendant, though conceding that its purpose was commercial, argued that its use was transformative. However,

"...although defendant recites that My.MP3.com provides a transformative "space shift" by which subscribers can enjoy the sound recordings contained on their CDs without lugging around the physical discs themselves, this is simply another way of saying that the unauthorized copies are being retransmitted in another medium--an insufficient basis for any legitimate claim of transformation...Here, defendant adds no new "new aesthetics, new insights and understandings" to the original music recordings it copies, but simply repackages those recordings to facilitate their transmission through another medium. While such services may be innovative, they are not transformative."¹⁶

How distinguishable are the facts in this case from those in *RIAA v Diamond*? In the latter case, the Rio player was utilised by its users to store audio recordings which the users had obtained, irrespective of whether those recordings were authorised or unauthorised MP3 versions of sound recordings. Arguably, the "space-shifting" activity is being done by an individual. Where Internet storage is concerned, it is equally available to an individual to store copies of his CD recordings, lawfully purchased, on the Internet: several sites offer free web spaces which can be utilised for such purposes. Had the defendant company merely intervened and facilitated the actual upload of the songs on behalf of its users, the court *may* have been, though not necessarily, persuaded of the "space-shifting" argument: however, what the defendant sought to do was something quite different. It placed sound recordings derived, not from users' CDs, but from another set of CDs which duplicated those of the users. Nevertheless, , can this not be argued to be a technologically different type of space-shifting? After all, only such users who are lawful purchasers of sound recordings have access to the defendants' storage site.

The court analysed the second and third factors more rapidly: sound recordings are creative works which are close to the core of intended copyright protection;¹⁷ and it was undisputed that the defendant had copied the entirety of the copyrighted works.

In relation to the four factor, the court felt that the defendant's activities invaded the plaintiffs' ability to license their sound recordings to others for reproduction. The defendants argued that its activities could only enhance plaintiffs' sales, since subscribers could not gain access to particular recordings made available by MP3.com unless they had already "purchased", or agreed to purchase their own CD copies of those recordings. Indeed, similar arguments were put forward by Napster in relation to whether its peer-to-peer activity harmed the recording industry's sales. As in Napster, the court here was not moved:

"Any allegedly positive impact of defendant's activities on plaintiffs' prior market in no way frees defendant to usurp a further market that directly derives from reproduction of the plaintiffs' copyrighted works."¹⁸

¹⁶ 92 F. Supp. 2d 349 (S.D.N.Y., 2000), at p. 351.

¹⁷ *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569 at p. 579 (S.Ct., 1994).

¹⁸ 92 F. Supp. 2d 349 (S.D.N.Y., 2000), at p. 352.

It is hard not to conclude that the court was, irrespective of the analysis concerning the four factors, convinced that the act was "unfair" - the defendant had utilised another work in order to gain income, in this case by means of advertising revenues. Imagine extrapolating this scenario to a trade mark case: defendant offers a site where goods of different traders are exhibited, with a set of prices. The service allows users to compare the different prices of competing traders. Nevertheless, the defendant is enjoined from utilising names of traders as a breach of trade mark or unfair competition protection. The argument is: you cannot use the property of another to your advantage. Can this be always true? Should not there be some flexibility of use of intellectual property works for the benefit of the consumer?

Indeed, the defendant attempted to state that its activity and web site provide a useful service to consumers which, in its absence, would be served by "pirates." The court replied, in what is perhaps a constitutionally interesting proposition, that copyright

"... is not designed to afford consumer protection or convenience but, rather, to protect the copyrightholders' property interests."¹⁹

CASE 3: NAPSTER

A small Internet start up company, founded in May 1999 by a 19-year old college dropout Shawn Fanning, revolved around a program which builds communities around types of music. Since going on-line in September 1999, the Napster site has raised \$15 million in venture funding, attracted over 20 million users, and facilitated the download of over 1400 songs per minute. In 1999, several major recording labels filed an action seeking damages and injunctive relief against Napster. Napster was not sued for direct infringement, due to the fact that the technology did not directly copy files on to its central server but merely allowed peer-to-peer sharing. Instead, it was claimed by the recording industry that Napster's peer-to-peer file-sharing technology and Internet directory service made Napster contributorily and vicariously liable for its users' alleged copyright infringement. Napster raised an assortment of defences for its conduct, including

- the fair use defence on the part of Napster users, including the *Sony* defence;
- the AHRA non-commercial user exceptions;
- the "safe-harbour" defence provided under the DMCA.

The Napster network allows music aficionados to, *inter alia*, make MP3 music files stored on individual computer hard drives available for copying by other Napster users; search for MP3 music files stored on other users' computers; and transfer exact copies of the contents of other users' MP3 files from one computer to another via the Internet. Napster's "peer-to-peer" architecture replaces the traditional method of using large centralised information servers to supply the requested files. Important factors in considering the technology are:

- Napster servers do **not** create, copy, store or make available any of the MP3 files on its servers (whether transient or otherwise);
- the contents of all MP3 files are held at all times on the users' computers;
- the contents of the MP3 files are **not** routed or transmitted through Napster's servers;

¹⁹ *Ibid*, at p. 352.

Napster merely holds a database of MP3 file names and, if requested, the IP address information of each user.

It is difficult to definitively categorise Napster: it can simultaneously be viewed as a service provider, a search engine, and a provider of information location tools such as directories or indexes.²⁰

Direct Infringement by Napster Users

In order to prove that Napster was liable for contributory and vicarious copyright infringement, the industry had to prove that Napster users themselves were actively engaged in the unauthorised reproduction and distribution of copyrighted works. In order to counter this claim, Napster had to prove that all or some of the activities indulged in by its users exempted them from the charge of direct infringement, under the fair use defence, and if this is the case, Napster itself could not be held liable. The district court held that the recording industry had presented a prima facie case of direct infringement by Napster users. In doing so, it accepted the industry's claim that more than eighty percent of the files available on Napster may have been copyright protected and owned or administered by plaintiffs, thereby violating the plaintiff's exclusive rights of reproduction and distribution under §106, U.S. Copyright Act.²¹ The Court of Appeal found nothing wrong in the district court's finding and Napster did not further argue this point. It instead relied on the fair use defence and claimed that it could avail itself of the "safe harbour" provisions under the DMCA.

What Does "Sharing" Entail?

Napster contended that users could not be considered to be direct infringers as they were engaged in fair use of the material. Both the district court and the appellate court concluded otherwise.²² The Court of Appeal emphasised the point of unfair dealing stating that, as opposed to direct economic gain by the users, the key issue was the "repeated and exploitative copying of copyrighted works, even if the copies are not offered for sale".²³ Another hotly disputed feature was whether Napster use harmed the market for copyright music. The district court held that Napster use harms the market for copyright musical compositions and sound recordings, especially in relation to sales within college markets (a high proportion of Napster users are students). The court rejected Napster's report which showed that Napster is beneficial to the music industry because MP3 music file-sharing stimulates more audio CD sales than it displaces. Market harm is viewed from the perspective of the current market and any potential market into which the copyright holder may have an interest in.²⁴ The district court determined that Napster had harmed the music industry's

²⁰ See arguments below in respect of the DMCA "safe harbour" defence.

²¹ *Napster*, 114 F.Supp.2d 896 (N.D. Cal. 2000), at p. 911.

²² *Napster*, 114 F.Supp.2d 896 (N.D. Cal. 2000), at p. 911; 239 F.3d 1004 (9th Cir. 2001), at p. 1015.

²³ *Napster*, 239 F.3d 1004 (9th Cir. 2001), at p. 1015.

²⁴ *UMG Recordings*, 92 F.Supp.2d at 352.

market in two ways: it reduces audio CD sales among college students and it raises barriers to plaintiffs' entry into the market for the digital downloading of music.²⁵ The Court of Appeal concurred with this finding, adding the that

"lack of harm to an established market cannot deprive the copyright holder of the right to develop alternative markets for the works

Space Shifting

What about "space-shifting"? This is where a user accesses and downloads an MP3 formatted sound recording through the Napster system in order to listen to music that she already owns in an audio CD format. As discussed above in the *RIAA v Diamond* decision, space shifting of musical compositions and sound recordings can be a fair use,²⁶ and this strand of defence stems from the *Sony* decision.²⁷ The district and appellate courts refused to apply the "shifting" analyses of *Sony* and *Diamond* to the MP3 decision on the basis that Napster based activities had an inherent distributive element within its users' activities. *Diamond* and *Sony* were distinguished in that the methods of shifting employed by the users did not also simultaneously involve distribution of the copyright material to the general public; the time or space-shifting of copyright material exposed the material only to the original user.

Conversely, it is obvious that once a user lists a copy of music he already owns on the Napster system in order to access the music from another location, the song becomes "available to millions of other individuals," not just the original CD owner.²⁸

The objection here revolves, once again, around the fact that Napster facilitates the downloading and distribution of music; whereas, the end destination in the case of *Diamond* and *Sony* hardware was the media storage device i.e. the Rio player and the Betamax VCR, respectively.

Contributory Liability

A party is liable for contributory infringement if he has knowledge of the infringing conduct of another, and induced, caused or materially contributed to the infringing conduct. Could Napster really be said to have encouraged and assisted in the infringement of the plaintiffs' copyright? Did it not have a disclaimer on its site and a specific injunction to its users against the download and distribution of copyright music? Finally, can knowledge be assumed to Napster? The district and appellate courts concluded that Napster had both actual and constructive knowledge that its users exchanged copyright music in spite of the fact that the plaintiffs' could not definitively identify more than 200 song titles.

²⁵ *Napster*, 114 F.Supp.2d 896 (N.D. Cal. 2000), at p. 913.

²⁶ *Recording Industry Association of America v. Diamond Multimedia Sys., Inc.*, 180 F.3d 1072 at p. 1079 (9th Cir.1999).

²⁷ *Sony Corp. v. Universal City Studios, Inc.*, 464 U.S. 417, at p. 423 ("time-shifting," i.e. where a video tape recorder owner records a television show for later viewing, is a fair use).

²⁸ *Napster*, 239 F.3d 1004 (9th Cir. 2001), at p. 1019.

What of the decentralised nature of peer-to-peer technology which prevents Napster from knowing the nature of their users' activity and of the files shared. The only information that Napster can access is to the user-given file names. First, these file names do not necessarily reveal whether the work is copyright protected or not. The situation is more difficult in the case of classical music as file names are usually identified by the composer and the name of the work (for example, Beethoven, 1st symphony, 2nd movement), without any indication as to the performers or the recording label.²⁹ Secondly, Napster does not control the file names and it is open for users to either inadvertently or deliberately misidentify their files: thus, an unknown artiste, in order to receive maximum publicity, may name his file:

"B. Spears, Oops, I did it again".

The technology does not enable Napster to determine whether this is an infringing file or not except by downloading and listening to all songs which appear to have potentially suspect file names on its servers. This confirms the fact that file names, *per se*, do not identify the artist or the song title, or whether the music is from a CD (in which event the Plaintiff recording companies may own the rights) or a recording of a live concert (which many artists allow to be freely circulated for promotional reasons). Moreover, programs such as Aimster allow users to circumvent Napster filters by automatically transcribing copyrighted song titles into Pig Latin.³⁰ Even the District Court agreed that it would be too "burdensome or even impossible to identify all of the copyrighted music they own"; instead, the court, in reliance on previous case-law, held that knowledge need not relate to "specific acts of infringement".

Nonetheless, it still held that the plaintiffs had demonstrated a likelihood of success in relation to material contribution. Relying on the district court's findings, the 9th Circuit held that without the support services that the defendant provides, Napster users could not find and download the music they wanted with the ease of which defendant boasts and that Napster provides "the site and facilities" for direct infringement.

CASE 4: DVD AND DECSS

Action was brought, under the Digital Millennium Copyright Act, by the film industry in *Universal City Studios v Reimerdes*³¹, to enjoin the Internet web-site owners from posting the DeCSS program and to prevent them from including hyperlinks from their site to others that similarly post the DeCSS program. On August 17, 2000, the United States District Court for the Southern District of New York entered judgement for Universal Studios against defendants for posting DeCSS technology. On appeal, the Court of Appeals for the 2nd Circuit upheld the lower court's decision in banning the publication of the DeCSS.³²

²⁹ Based on author's own research usage of the Napster system on 28th May 2001.

³⁰ Reported in Newsbytes.com, <http://www.newsbytes.com>, 24 May 2001.

³¹ 111 F.Supp.2d 294 (S.D.N.Y., 2000).

³² *Universal City Studios, Paramount Pictures Corporation, MGM Studios Inc., Tristar Pictures, Inc., Columbia Pictures Industries, Inc., Time Warner Entertainment Company, L.P., Disney Enterprises Inc., Twentieth Century Fox Film Corporation, v. Eric Corley and 2600 Enterprises Inc.* (United States of America, Intervenor).60 U.S.P.Q.2d 1953 (2nd Cir, 2001). The Court of Appeal gave a short judgement in relation to the copyright issues, agreeing substantially with the District Court's opinion. The 2nd Circuit court chose, instead, to focus on the First Amendment aspects of the case.

The film industry currently issues and distributes many of its copyright protected films for home use in digital form on five-inch wide disks which are capable of storing between 4.3 to 6 GB of data - DVDs (digital versatile disks).³³ The DVD technology affords drastically improved audio and visual clarity and quality of films, which can be viewed on televisions or computer screens. Unlike the music industry, the film industry awaited until their copyright protection technology was in place before introducing DVDs on the consumer market. Nearly all DVDs, since 1997, are protected from copying by using an encryption system called CSS (Contents Scramble System), which only allows for films to be viewed on players and computer drives equipped with licensed technology that permits the devices to decrypt and play (but not to copy) the films.

In 1999, three computer programmers reversed engineered a licensed DVD player and discovered the CSS encryption algorithm and keys; utilising this information, they invented the DeCSS program that enables users to break the CSS copy protection system and view DVDs on unlicensed players. The DeCSS further allows the user to make digital copies of films with little or no visible degradation to the quality of the work.³⁴ The defendants, Reimerdes and Corley, posted DeCSS on their Internet web site and provided links to other DeCSS sites. A further technological device which illustrates the film industry's concern is the DivX technology. DivX is to video files as MP3 is to audio files: the DivX technology can compress a 6 GB video file to 650 MB and is utilised often to facilitate either the transfer of video files to writeable CD-ROMS (which have an upper capacity of 650 MB) or the transfer of video files over networks. The plaintiffs' evidence demonstrated that Internet users were exchanging films in compressed, decrypted formats.³⁵

The main aim of the DeCSS program is dependent on the perspective one takes. Consider the following descriptions by counsel for both parties during the appellate hearing:³⁶

"DeCSS simply allows you to liberate the encrypted content for a variety of uses, some of which are perfectly innocent under the copyright laws, fair uses or non-infringing uses, and others of which might speculatively be copyright infringements",

or

"DeCSS was created for the sole purpose of ripping open DVDs so that would-be fair users perhaps, infringers more likely, can make copies of these films... they don't just make a copy, they make a perfect copy. And then they are able to take that perfect copy and put it on the Internet and distribute it worldwide."

³³ *Universal City Studios, Inc. et al v. Shawn C. Reimerdes et al*, 111 F.Supp.2d 294 (S.D.N.Y., 2000), at pp. 307, 313.

³⁴ *Ibid*, at p. 308.

³⁵ *Ibid*, at pp. 314-315.

³⁶ Transcript of oral hearings in *Universal City Studios, et al v. Reimerdes et al, (with the United States of America as Intervenor)*, 2nd Cir, May 1, 2001, Case No. 00-9185.

There are two main defences:

- i) the DMCA should not be construed to encompass the defendants' conduct since such a construction would also prevent those who wish to gain access to technologically protected copyrighted works in order to make fair use of them;
- ii) the DMCA, as applied to computer programs or code, violates the First Amendment.

Balancing Fair Use & Anti-Circumvention Devices

§1201(a)(2), DMCA reads:

"No person shall ... offer to the public, provide or otherwise traffic in any technology ... that--

- (I) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under [the Copyright Act];
- (II) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under [the Copyright Act]; or
- (III) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under [the Copyright Act].

Briefly, §1201(a)(2) allows, where a work is encrypted, the copyright owner to enjoin any person who distributes any anti-circumvention or decryption device to unlock the work. Was the DeCSS designed primarily to circumvent CSS? The district court held that, from the testimony of the witnesses, this was all it was meant to do, and that the defendants were in breach of §1201(a)(2). In thus holding, the court rejected the "Linux Argument" that the DeCSS was not created for the purpose of pirating copyright motion pictures but rather it was written to further the development of a DVD player that would run under the Linux operating system (there were no Linux compatible players on the market at the time). The court held that the question whether the development of a Linux DVD player motivated those who wrote DeCSS is immaterial to the question whether the defendants violated the anti- trafficking provision of the DMCA.

The second charge relates to whether linking to another web site containing the DeCSS program constitutes offering of or trafficking in anti-circumvention devices under the DMCA. The defendants had initially posted the DeCSS program on their web site; although the [FN F03333](#) defendants were forced to remove the program from their web site under a preliminary injunction, they continued to, in what was termed an act of "electronic civil disobedience," support nearly 500 hyperlinks on their web site to other sites purporting to offer DeCSS for download.³⁷

The extent to which §1201(a)(2) caught their activity depended on the nature of the links that defendants established on their web site. Some links transferred the user to a web page which does not contain a link to DeCSS, but links to another page on the same site that posts the software: in such a case, it is up to the user to follow the link or series of links on the linked-to web site in order to arrive at the page with the DeCSS link and commence the download of

³⁷ *Universal City Studios*, 111 F.Supp.2d 294, at p. 312.

the software. Other links take the user to a web site on which there appears a direct link to the DeCSS software: the user has only to click on the DeCSS link to commence the download. Still other links directly transfer the user to a file such that the download of DeCSS to the user's computer automatically commenced without further user intervention.³⁸

It was held that the defendants' links to sites that automatically commenced the process of downloading DeCSS and to web pages that displayed nothing more than the DeCSS code or present the user only with the choice of commencing a download of DeCSS, were "the functional equivalent of transferring the DeCSS code to the user themselves."

However, what of links which merely transferred one to a contents rich site which happened to also offer a hyperlink for downloading, or transferring to a page for downloading, DeCSS. For example, what if the Los Angeles Times site carried a link to a site which contained the DeCSS code: would the LA Times be liable, and would anyone else who linked *their* page to the LA Times be liable, regardless of the purpose or the manner in which the link was described? Would the La Times be held to have "offered, provided or otherwise trafficked in DeCSS" merely because DeCSS happened to be available on the site. Having asked the question, the district court deliberately avoided offering an answer. It merely stated that the LA Times situation was not the one before it: it appeared that the defendant's conduct in "civil disobedience" was sufficient for the court to conclude that the links to contents-rich sites was a further violation of the DMCA.

The DMCA Defences

The key provisions relied on by both parties were §§ 1201(f), 1201(g)(4), and 1201(j), of the Digital Millennium Copyright Act.

Reverse Engineering

The first defence claimed under the DMCA is §1201(f) which provides that one may circumvent, or develop and employ technological means to circumvent or access control measures in order to achieve interoperability with another computer program provided that doing so does not infringe another's copyright. In addition, one may make information acquired through such efforts available to others, if the person in question provides such information solely for the purpose of enabling interoperability of an independently created computer program with other programs, and to the extent that doing so does not constitute infringement" - in other words, reverse engineering is allowed to a certain extent. The defendants contended that DeCSS is necessary to achieve interoperability between computers running the Linux operating system and DVDs .

The district court rejected this argument for the following reasons:

the provision only allows information acquired through reverse engineering to be made available by the person who acquired the information: the defendants did not do any reverse engineering but merely posted the program DeCSS which was taken from another web site;

the right to make the information available extends only to dissemination "solely for the purpose" of achieving interoperability and clearly does not apply to public dissemination;

³⁸ *Ibid*, at p. 325.

the creators of DeCSS cannot credibly maintain that the "sole" purpose of DeCSS was to create a Linux DVD player since DeCSS was developed on and runs under Window, which is a far more widely used operating system. Here, Judge Kaplan imputed knowledge on the part of the developers of DeCSS: they knew that DeCSS could be used to decrypt and play DVD movies on Windows as well as Linux machines; they knew that the decrypted files could be copied like any other unprotected computer file.

Encryption Research

The second defence was in relation to encryption research which is allowed under §1201(g)(4). This provision allows one to develop and employ technological means to circumvent a technological measure for the sole purpose of performing acts of good faith encryption research and to provide the technological means to another person with whom he is working collaboratively for the purpose of conducting such acts of good faith encryption or for the purpose of having that other person verify his acts of good faith encryption research. However, for the encryption defence to work, the person must have lawfully obtained the encrypted copy, and must show that he has made a good faith effort to obtain authorisation before the circumvention; and that the act does not constitute infringement under the DMCA. The district court's curt response to this plea was that neither of the defendants were involved in good faith encryption research as they had posted DeCSS for all the world to see; there was also no evidence that they made any effort to provide the results of the DeCSS effort to the copyright owners.

Security Testing

The third DMCA-related defence was in relation to security testing exempted under §1201(j): the exception however is limited to "assessing a computer, computer system, or computer network, solely for the purpose of good faith testing, investigating, or correcting [of a] security flaw or vulnerability, with the authorisation of the owner or operator of such computer system or computer network." The district court rejected this immediately holding that the DeCSS had nothing to do with testing computers, computer systems, or computer networks.

Fair Use and the Rights of Society

A second major contention was in relation to the DMCA's extension of content control. The defendants argued that the DeCSS program was a device which enabled users to circumvent technologically protected copyrighted works so as to make lawful use of those works. An interesting question arises as to whether a purchaser of a DVD is allowed to tamper with the copy protection device in order to play the file in a different computing environment.³⁹ The potential uses of the DeCSS program is linked to the primary issue: does the CSS encryption program have a significant utility in preventing infringement only, or does it go further and

³⁹ The court was unimpressed since the DeCSS is actually a Windows executable file and not a Linux file. The inventor explained that he created a Windows rather than a Linux program by asserting that Linux did not support the file system used on DVDs. Hence, it was necessary to decrypt the DVD on a Windows computer in order subsequently to play the decrypted files on a Linux machine, *Universal Studios*, 111 F.Supp.2d 294 (S.D.N.Y., 2000), at p. 311.

act as a significant bar to fair use and other non-infringing uses? Consequently, is the copy-protection system in itself harmful to both copyright law and the First Amendment right?⁴⁰

Judge Kaplan, in the district court, recognised that technological control measures present a legal paradox. They are important in that they secure protection for copyright owners who have made their works available in a digital format, since such works are easily copied and transmitted. On the other hand, such measures have the added ability to prevent fair uses of copyright works, thereby unjustifiably extending the ambit of copyright law. Nevertheless, Judge Kaplan accepted that the DMCA constituted a Congressionally-approved balance in this dilemma, and that the defendants' posting of DeCSS violated, without question, the DMCA. In other words, it was not up to him to question the inherent conflicts between the DMCA and the basis of copyright protection.

Moreover, the defendants in this case were not being sued for copyright infringement but for offering and providing technology designed to circumvent technological measures, thereby violating §1201(a)(2), DMCA.

"If Congress had meant the fair use defense to apply to such actions, it would have said so. Indeed, as the legislative history demonstrates, the decision not to make fair use a defense to a claim under Section 1201(a) was quite deliberate."⁴¹

The defendants also claimed that DeCSS might be used for the purpose of gaining access to copyrighted works in order to make fair use of those works, thus making the *Sony* defence applicable. However, the district court firmly held to the contrary opinion:

The question here is whether the possibility of noninfringing fair use by someone who gains access to a protected copyrighted work through a circumvention technology distributed by the defendants saves the defendants from liability under Section 1201. But nothing in Section 1201 so suggests. By prohibiting the provision of circumvention technology, the DMCA fundamentally altered the landscape. A given device or piece of technology might have "a substantial noninfringing use, and hence be immune from attack under *Sony*'s construction of the Copyright Act--but nonetheless still be subject to suppression under Section 1201." Indeed, Congress explicitly noted that Section 1201 does not incorporate *Sony*.... The fact that Congress elected to leave technologically unsophisticated persons who wish to make fair use of encrypted copyrighted works without the technical means of doing so is a matter for Congress unless Congress' decision contravenes the Constitution, a matter to which the Court turns below.⁴²

Thus, the district court clearly held to the view that the DMCA's intention was clearly to curtail the effects of the fair use doctrine in relation to encrypted copyright material.⁴³ The

⁴⁰ Per Judge Newman, oral argument in *Universal City Studios, et al v. Reimerdes et al*, (with the *United States of America as Intervenor*), before the 2nd Circuit Court of Appeals, New York, NY, on May 1, 2001, Case No. 00-9185.

⁴¹ *Universal City Studios*, 111 F.Supp.2d 294 (S.D.N.Y., 2000), at p. 322.

⁴² *Universal City Studios*, 111 F.Supp.2d 294 (S.D.N.Y., 2000), at p. 323-324.

⁴³ The fair use defence may be applicable under §1201.

only objection would be a constitutional one - which is discussed below.

However, can the picture be presented in such black and white terms? The problem arises in that both parties dispute the extent to which copyright protection systems control the user. For example, in the case of an individual user of a digital audio tape, the AHRA allows, as we have discussed above, such users to make copies for non-commercial private purposes. If the user of a digital audio tape can make an identical digital copy without infringing copyright law, then why cannot the user do the same act in relation to a digital video disc? Counsel for the intervenor (the U.S. Government) argued before the appellate court that the rationale for not allowing an individual user the same rights in relation to DVDs was that content providers would be bereft of any protection in light of the technologically changed environment - i.e. the Internet is more of a factor today than it was at the time of AHRA.

The appellate court, during oral arguments, was resistant to the idea that preventing access to DeCSS prevented fair use.

"I don't think it even does that. At best - at worst, it eliminates the fair uses in the most technologically preferable form, namely the digital rendering of the material. That's the worst it does. It doesn't say anything about making fair use with less technically excellent methods, right?"

In other words, the fair use principle does not call for the optimal method of utilising or downloading a work. This was countered by the defendants' counsel stating that the right to fair use encompassed more than the mere right to use a work in some form even though it was in a technologically inferior form. She argued that it

"encompassed the right to use something in the exact form by which the creator embodied it so long as the use is fair, so long as it's subject to all the limitations of the Copyright Act. What this Act does is shift a bargain that has been maintained and without this bargain, it's not clear that copyright itself would be defensible against First Amendment challenge. It can't be that the bargain is shifted all in favor of the property holder so that fair users are now condemned to use inferior technologies. I just want it to be clear there are also non-infringing uses. If your daughter were autistic and intended to destroy the home DVD collection because of her illness, it would be a non-infringing use for you to just back up the copy onto your hard drive under the Copyright Act, but this law would prevent you from using DeCSS to do that. And as you mentioned, scientific researchers - 1201(a)(2) as interpreted by the District Court, would prevent scientific researchers even under the statutory exceptions from using DeCSS to then post information about decryption and encryption in their own websites, or even to deliver lectures at Princeton or other places about their findings."

On the other hand, the appellate court was concerned as to whether the bar under the Copyright Act, as to the manufacture and distribution of decryption devices, would curtail the development of decryption programs in order to use works that fell into the public domain in the future.

Does the DMCA Forbid Fair Use?

The defendants' further contended that §1201(a)(2) is unconstitutional because it prevents others from making fair use of copyrighted works by depriving them of the means of circumventing plaintiffs' access control system: those who lack sufficient technical expertise to circumvent CSS themselves without the means of acquiring circumvention technology

would never be able to make fair use of the content of plaintiffs' copyrighted DVDs.[FN F237235](#)

The district court agreed that the anti-trafficking provisions probably did curtail fair uses of copyright materials on DVDs, but the effect was trivial. Irrespective of the type of fair use envisaged (for example, making a criticism, playing a portion of the musical sound track or broadcasting a section of the movie for purposes of review), since all or substantially all films available on DVD are available also on videotape. Therefore, fair use was preserved in relation to a different format of the copyright work, and anyone could buy or rent a videotape, play it, and even copy all or part of it with readily available equipment.

What if movies were available only on DVDs, as someday may be the case? The court insisted that the impact on lawful use would still be limited

as compliant DVD players permitted one to view or listen to a DVD movie without circumventing CSS in any prohibited sense. The technology permitting manufacture of compliant DVD players is available to anyone on a royalty-free basis and at modest cost, so CSS raises no technological barrier to their manufacture. Hence, those wishing to make lawful use of copyrighted movies by viewing or listening to them are not hindered in doing so in any material way by the anti-trafficking provision of the DMCA."

In other words, should the world be dominated by CSS-protected DVDs, fair use was to be limited to viewing or listening. The district court acknowledged that copying for fair use would be curtailed but dodged the query by stating that there were different types of fair uses within different types of communities, and that the question of constitutionality could not really be decided *in bloc*, without consideration of the circumstances of each user.

CASE 5: KABUSHIKI KAISHA SONY COMPUTER ENTERTAINMENT V. EDDY STEVENS (FEDERAL COURT OF AUSTRALIA)

Australia has made amendments to the *Copyright Act 1968* by the *Copyright Amendment (Digital Agenda) Act 2000*. Section 116A of the Copyright Act, which was introduced by the Digital Agenda Act, gives a right of action to the owner or exclusive licensee of the copyright in a work or other subject matter which is protected by a **“technological protection measure”**. The right of action is against a person who makes, sells, or does certain other acts in relation to, a “circumvention device” capable of circumventing, or facilitating the circumvention of, the technological protection measure.

The Sony companies (“Sony”) manufacture and sell PlayStation games which are capable of being played on ordinary domestic television sets by means of a PlayStation console, which Sony also manufactures and sells. The games are embodied in computer programs which are contained in CD-ROMs (“CDs”). Sony owns the copyright in the computer programs. Insertion of a PlayStation CD into the PlayStation console enables the game to be played.

There is an “access code” contained within a track on each CD, and a chip described as a “Boot ROM” is located on the circuit board of the PlayStation console. They have the effect that a game can be played only with the authority of the owner or licensee of the copyright. The reason is that an unauthorised copy of a Sony PlayStation CD does not replicate the

access code and therefore the Boot ROM of the console denies it access: it cannot be used in the console.

The respondent, Mr Stevens, sold “mod chips” or “converter chips” and installed them in PlayStation consoles. Their purpose and effect was to overcome Sony’s device. But they would constitute “circumvention devices”, and Sony would have a right of action against Mr Stevens under the new s 116A, only if Sony’s device itself constituted a “technological protection measure” as defined in subs 10(1) of the Copyright Act.

The first instance court held that it did not on the grounds that the definition required that in order to be a technological protection measure, a device must be designed to prevent or inhibit post-access infringement of copyright. The Federal Court disagreed holding that it was sufficient that Sony’s device inhibits infringement by rendering the resulting unauthorised copies unusable.

The full text of the Court’s judgment, reported as *Kabushiki Kaisha Sony Computer Entertainment v Stevens* [2003] FCAFC 157, is available on the Court’s website at www.fedcourt.gov.au.

[End of document]