IRIS plus
LEGAL OBSERVATIONS
OF THE EUROPEAN AUDIOVISUAL OBSERVATORY

Movies Online: Balancing Copyrights and Fair Use

Less than two years ago, our *IRIS Focus* featured an article that reported on a first wave of lawsuits related to online offers of audio files (see IRIS 2000-8: 14, "MP3: Fair or Unfair Use?"). By then it had already become a question of time when digital technology would have sufficiently progressed to make the supply of audiovisual files over the Internet equally attractive.

Meanwhile movies have gone online and, as was to be expected, they are mainly offered without the consent of the copyright holders. In addition, they are offered in circumvention of technological measures for copyright protection. Accordingly, providing movies online evokes familiar and new legal issues. As in MP3 cases, the United States' industry is at the forefront of litigating these issues in court. The legal problems related online movie services, however, are of a truly global nature.

This IRIS *plus* supplements our earlier article by focusing on the new legal questions as well raised as their factual background. Thereby, we hope to cater to your needs for legal information and for knowledge of the underlying technological developments.

Strasbourg, April 2002

Susanne Nikoltchev
IRIS coordinator
Legal expert of the European Audiovisual Observatory

IRIS *plus* is a supplement to **IRIS,** *Legal Observations of the European Audiovisual Observatory,* **Issue 2002-4**

OBSERVATOIRE EUROPÉEN DE L'AUDIOVISUEL
EUROPEAN AUDIOVISUAL OBSERVATORY
EUROPÄISCHE AUDIOVISUELLE INFORMATIONSSTELLE

76 ALLEE DE LA ROBERTSAU • F-67000 STRASBOURG
TEL. +33 (0)3 88 14 44 00 • FAX +33 (0)3 88 14 44 19
http://www.obs.coe.int
e-mail: obs@obs.coe.int

IRIS plus LEGAL OBSERVATIONS OF THE EUROPEAN AUDIOVISUAL OBSERVATORY

Movies Online: Balancing Copyrights and Fair Use

by **Susanne Nikoltchev & Francisco Javier Cabrera Blázquez**
European Audiovisual Observatory

Introduction

The digital versatile disc (DVD) is the standard digital medium, agreed upon by all major movie studios, for home distribution of movies. A DVD has a diameter of five inches and is capable of storing several Gigabytes of data and, thus, holding cinema-like video in the form of digital audio-visual files. DVDs can be played by DVD players or on PCs equipped with DVD-ROM drives and additional hardware or software modules (media players).

Today the technically versed is likely to succeed in separating a movie file from the DVD, its original carrier. Hence, he can produce identical copies by simply duplicating the digital information onto the hard drive of his computer. From then on the movie is, like any other file, readable from the PC's hard drive and it is e-distributable. Should the movie file be offered on the Internet, anybody can make his own copy. While this process entails almost no costs or effort, it does give rise to legal issues concerning the intellectual property rights of the movie and the DVD industry. Though still in its infancy, the DVD market has gained in significance[1] and the major market players are keen to use whatever means they can, including litigation, to guard it against piracy.

In our previous publication "MP3: Fair or Unfair Use"[2] we have already treated key legal questions such as whether the copying of a digital file from a CD onto an electronic carrier is a violation of copyright laws, what instances of copying might be allowed, or what are the implications of existing distribution schemes. The factual and legal problems arising from the illicit copying and distribution of digital movie files resemble largely that for CDs because the principal technology of MP3[3] is the same as that for digital versions of movies. Consequently, individuals can offer digital copies of DVD movies (as done already with CD recordings) directly on their web sites or hyperlink to such copies stored elsewhere. They can provide special distribution schemes[4] or link to such schemes hosted on other web sites.

As a more recent development, captured by the MP3 article only in its early stage, individuals can now participate in peer-to-peer networks, which shakes up some of the relevant legal considerations. Peer-to-peer systems operate with the snowball effect: a user first connects to one or more other users in order to launch his request for a specific movie; the recipients then forward this request to their connections until the corresponding electronic file is found within the network. Finally, the transfer of the file takes place between two private parties and remains anonymous.[5] Lately the exchange of movie files over the Internet has been facilitated and accelerated by the "FastTrack" system, which builds on a new variant of the peer-to-peer file sharing software and is offered free of charge on the Internet. The resulting litigation illustrates how MP3 litigation has found its continuation in peer-to-peer distribution schemes for movies.

The Internet exchange of film files, however, raises legal issues that go beyond those litigated for MP3 and even beyond those added by FastTrack. This is mainly because the industry put a technical safeguard, called Content Scramble System (CSS), against illegal copying on DVDs that was not yet of relevance for CDs in the MP3 example.[6] The reply by some programming experts followed promptly in form of DeCSS, software that can unscramble CSS.

The mixture of *déjà vu* and new aspects concerning the distribution of digital audio-visual files determines the structure of this article. It starts with the litigation surrounding MP3 thereby pinpointing those legal issues that bear on the dissemination of digital movie files. Thereafter, it focuses on the FastTrack litigation, describes the CSS/DeCSS technology with its legal implications and ends with a short conclusion.

Lessons to Be Learned from Audio Litigation

If any transfers of digital audio or audio-video files happen without the consent of the copyright holder, litigation is likely to follow. This was the case with Internet distribution of MP3 and now happens with regard to the electronic transfer of movie files. So far the MP3 case law indicates that it is illegal to offer unauthorised audio files to unspecified customers irrespective of whether this is done through linking directly to these files, to file listings, or to other web sites that provide direct links or listings. Furthermore, Internet Service Providers whose services are required for the online exchange of MP3 files and the hosting of web sites risk being liable for indirect copyright infringement at least in some countries.[7]

MP3 litigation also addressed copyright protection with regard to specific distribution schemes such as the "My.MP3.com"[8] and "Napster"[9] services. The My.MP3.com service permitted subscribers to store, customise, and listen to recordings contained on their CDs from anywhere in the world if they had access to the Internet. The digital copies replayed for the customer were made and archived by the company offering the service and mostly they were not authorised. By contrast, the Napster distribution system functioned merely as a platform for the exchange of MP3 copies between its customers. Except for the index of available files that Napster provided, it was basically a peer-to-peer system. My.MP3.com and Napster services were banned in the US, though in the Napster case only by a preliminary ruling pending a decision on the merits.

Whatever the claim was, the courts first had to establish direct copyright infringement. They seemed at ease with ascertaining the necessary facts whenever a major part or all of the MP3 files offered over the Internet had been copied without the consent of the copyright holder.[10]

The more difficult question was whether the up- or downloading could be justified as private or fair use or under any other exception. On one occasion, freedom of expression was (unsuccessfully) invoked with the argument that banning links to MP3 files was an undue restriction.[11] In a similar direction points Napster's claim that plaintiffs had colluded to "use their copyrights to extend their control to online distribution".[12]

The balancing of absolute copyrights against the public interest in some private use (or in US terminology "fair" use) was not only at the centre of MP3 litigation, but it had already been an issue at the First WIPO Diplomatic Conference in 1884.[13] Ever since, exceptions to absolute copyrights were written into international treaties and national laws. The most recent relevant statutory addition to European legislation is the Directive on Copyright in the Information Society ("Directive").[14] Article 5 of the Directive enumerates all exceptions and limitations to copyrights for which domestic legislation may – though not must – provide.[15] The private use exception is expressly envisaged for the reproduction right in Article 5 para. 2. (b), if non-commercial ends are pursued. It is referred to in connection with the distribution right in Article 5 para 4. Private use applies with regard to digital carriers and therefore covers private copying onto hard drives. It is irrelevant whether the individual making a private copy does so for his personal use or for use by a third person.[16] Private use – as with all other exceptions to copyrights under EC law – is further limited to "certain special cases which do not conflict with a normal exploitation of the work or subject-matter and do not unreasonably prejudice the legitimate interests of the rightholder." Different from other exceptions and different from fair use, private use generally presupposes that the rightholder receive fair compensation

Fair use played the leading role in judging the acts of users of My.MP3.com and Napster services. Different from the European approach where private use is framed by key elements that are further elaborated and fixed in domestic law, fair use is to be determined dynamically on a case by case basis. Whilst, according to 17 U.S.C. § 107, four specific factors must be taken into account, others might be considered as well. This is again different from the EC law.

In the MP3 cases, none of these factors had been met. For Napster, however, this is still only a preliminary conclusion and so far the US boundaries of "fair use" have not finally been settled.

Regarding specific distribution schemes, examining copyright infringement does not stop with finding customers primary liable for up- or downloading electronic files. The next question is whether the service provider can be held liable as well. The Napster service provider was found to be secondarily liable for direct copyright infringement in accordance with the doctrines of contributory and vicarious copyright infringement.[17]

Napster challenged the finding of secondary liability under § 512 (a) of the Digital Millennium Copyright Act ("DMCA").[18] This safe harbour provision limits liability for online service providers with regard to information exchanged through their services if the provider supports technical copyright protection measures such as scrambling systems. It is inapplicable if he knew or had reason to know about (repeated) infringements. The likelihood of knowledge killed Napster's defence in the preliminary proceeding where the preceding question of whether Napster was an Internet Service Provider at all remained open. It appears that schemes for the distribution of digital files via the Internet might meet the DMCA safe harbour provisions. Should they not yet satisfy the requirements, some alterations in the technical setting could tip the balance in their favour. This might already be the case for the peer-to-peer constellation.

In comparison, the Directive comes into line with this result. On the one hand, it introduced the exclusive right of making available that Member States must provide for producers of first fixations of films with regard to originals or copies of their films. Centralised distribution schemes, like those used for MP3, offer services that "members of the public can access from a place and at a time individually chosen by them".[19] Therefore, they are likely to qualify as interactive on-demand transmissions. Consequently, these services might clash with the right of making available unless the use were authorised by the copyright holder. On the other hand, Consideration (27) of the Directive stipulates that "the mere provision of physical facilities for enabling or making a communication does not in itself amount to communication within the meaning of the Directive." This suggests that at least the "traditional" Internet Service Provider is safe from liability for rendering his services. How Napster would be judged is uncertain because peer-to-peer networks appear to be an interesting in-between case.

The FastTrack System: MGM v. Grokster

The most successful of these peer-to-peer ("P2P") networks has been created through the FastTrack system, which is proprietary P2P file-sharing software. FastTrack permits each of its users to locate any kind of computer files held by any other user and to obtain a copy through an individual transfer directly from user to user (without a centralised server). The Consumer Empowerment BV (also known as "Kazaa") developed the FastTrack software, distributed it free of charge over the Internet, and licensed it to Grokster and MusicCity. Subsequently, both enterprises offered FastTrack likewise free of charge on the Internet. Each of the three companies offers FastTrack with its own interface and uses it to display messages and advertisements. FastTrack enables Kazaa, Grokster and MusicCity to share the same network of users.

FastTrack works like other P2P systems, but unlike them it is not completely decentralised. In fully decentralised P2P file-sharing networks (like Gnutella) search queries must often go through the whole network because every computer is being asked for the desired file. This creates not only a huge amount of Internet traffic but also slows down considerably the searching process (or even renders it impossible on occasions).

In order to avoid this problem, the creators of FastTrack designed the SuperNode network system. SuperNodes may be imagined as a random selection of user computers designated to function as a "turntable" for a specific geographic area of FastTrack users. Apparently, the system chooses the individual computers used as SuperNodes automatically and changes them constantly according to the network needs. Users must consent to be appointed as SuperNodes.

Each user connects to a specific SuperNode, which "controls" a series of users and keeps an index of their files available for downloading. All SuperNodes are connected among themselves and thereby linked to the indexes of each of them. As a network, the SuperNodes administer a combined list of all files available from all FastTrack users. By contrast, a Napster like system would operate an index of files through one or several central servers. By contacting his "local" SuperNode a FastTrack user automatically calls on all SuperNodes' lists for his search.

On 2 October 2001, Plaintiffs representing the recording and film industry filed a complaint for damages and injunctive relief for copyright infringement against Grokster, Ltd., MusicCity.Com, Inc., MusicCity Networks, Inc., and Kazaa.[20] The case goes to jury trial on 1 October 2002.[21] The Plaintiffs brought this action "to stop Defendants from continuing to encourage, enable, and profit from the massive infringements of Plaintiffs' copyrighted works on the Internet".[22] The Defendants' actions were allegedly "willful, intentional, and purposeful, in disregard of and with indifference to Plaintiffs' rights". According to the Plaintiffs, the majority of the digital files found on the Defendants' network are illegal, including recently released films, some of them still playing in cinemas and not yet available on the video/DVD or television market.

The Defendants concede that users of their network have engaged in unauthorised distribution of copyrighted works. This case is therefore solely about the secondary liability of Defendants for direct infringement under contributory copyright infringement and vicarious copyright infringement.

Contributory Infringement

The doctrine of contributory copyright infringement establishes that "one who, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another, may be held liable as a 'contributory' infringer".[23] According to the Plaintiffs, the Defendants provide the software, support and services for the infringements, therefore assisting and facilitating them and they encourage users to engage in such conduct.

Regarding Napster, the Court of Appeals had held that without the support services provided by Napster, users could not have engaged in the unauthorised reproduction of copyrighted material through its network. Yet it stated that merely supplying the means to accomplish an infringing activity would not have amounted to contributory infringement. However, because Napster's central servers operated the index of files, Napster had actual knowledge of infringement activities in its network yet neglected to prevent the unauthorised copying of music files. Therefore, the Court concluded, Napster materially contributed to the infringing activity.

In contrast to Napster, the Defendants allege that they lack (upon delivery) actual knowledge of how customers will use their software. They claim not to participate in the process of searching or exchanging files within the network because the SuperNodes jointly operate the file index. Moreover, they contend neither to receive any information about search activities nor to have any knowledge of such activities.

The Plaintiffs counter that they have notified the Defendants of infringing files. In addition, users would be freely talking about their infringing activities in a chat room monitored by the Defendants.

The Defendants also invoke the Sony Betamax rule,[24] which stipulates that "the sale of copying equipment, like the sale of other articles of commerce, does not constitute contributory infringement if the product is widely used for legitimate, unobjectionable purposes. Indeed, it need merely be capable of substantial non-infringing uses". The Defendants contend that, like the Sony Betamax video recorder, the FastTrack software is capable of substantial non-infringing uses.

The Plaintiffs contest this defence because the Defendants designed their software for infringing use and Sony Betamax neither shields the unauthorised distribution of copyrighted works nor applies when the infringing activity can be blocked while permitting non-infringing uses to continue. According to the Plaintiffs, the Defendants failed to demonstrate the significant non-infringing uses.

Vicarious Infringement

A vicarious infringer "has the right and ability to supervise the infringing activity and also has a direct financial interest in such activities".[25] He need not be aware of the actual infringement. According to the Plaintiffs, the Defendants became vicariously liable because they exert control over the means by which the direct infringement occurs. They benefit from these illegal acts by drawing users to the network and derive financial advantages by displaying advertisements on their software interfaces.

According to the Napster case, financial benefit lies where the availability of infringing material "acts as a 'draw' for customers."[26] In the present case, financial gain seems to be even more pointed because the Defendants obtain revenue for displaying advertisements. Their fees depend on the number of network users.

Instead of the Sony Betamax rule, which is restricted to contributory infringement, the Defendants invoke their inability to monitor and/or control users' activities after delivery of the P2P software. They claim that even if they were to shut down their central servers, the whole system would continue to function. Only, usernames would not be properly displayed on the interface, and graphics and advertisements would not appear on the screen. The Plaintiffs contest this defence, stressing the Defendants' efforts in updating and maintaining the software as well as fostering their relationship with clients.

"In the wake of the Napster decision, it appears that copyright law has foisted a binary choice on P2P developers: either build a system that allows for thorough monitoring and control over user activities, or build one that makes such monitoring and control completely impossible".[27] Kazaa, Grokster and MusicCity seem to have learned this lesson when they developed a business model based on a self-generated network administered by SuperNodes, which possibly shields them from secondary liability for copyright infringement. Yet the attacks on this system launched by the Plaintiffs must still be repelled. The Jury's key question will be whether the Defendants had actual knowledge of the infringing activities and whether they could have effectively monitored or controlled them.

The similarities between the Napster and FastTrack distribution schemes should not blind us to those elements that set audio and audio-visual files apart. Notably, DVDs from the very start enjoyed a higher level of technical protection. The motion pictures companies developed and introduced an access control and copy prevention system to safeguard against illegal copying. This system added another legal dimension to the copyright litigation.

The CSS and DeCSS

The "Content Scrambling System"(CSS) controls access to digital movie files and prevents their copying. It is a two-tier protection system that employs a series of keys stored on the DVD and the DVD player to validate the authenticity of both.

First, CSS encrypts sound and graphic files. To this end, every DVD disc on the market is coded with an encrypted "disc key", identifying that disc. Second, the hardware (DVD player or a computer DVD drive) is equipped with a matching configuration so that it can decrypt, unscramble and play back the scrambled information. When a DVD player attempts to read a DVD, the player uses its player key and proceeds down the list of encrypted disc keys on the disc, trying to decrypt one that matches that on the DVD. The player key is validated once a correct disc key is found and another key for the DVD becomes available. This key then serves to actually unscramble the DVD content.

CSS permits the playing devices to decrypt and play – but not to copy – the films. The DVD Copy Control Association (DVDCCA) provides the CSS keys and licenses them to manufacturers of discs and players subject to strict security requirements. The licence also prohibits manufacturing equipment that would supply digital output usable in copying protected DVDs.

For the time being CSS is compatible only with computers using the Windows – but for example not the Linux – operating system.

In the 21st century it appears almost inevitable that a scrambling system finds its "unscrambler". This holds even truer where the incentives for decrypting digital information span from meeting the "scientific challenge" to accessing Hollywood movies at zero costs. In 1999, teenager Jon Johansen broke the CSS system by reverse-engineering a licensed DVD player. Based on the uncovered CSS encryption algorithm and keys, he developed a computer programme, called "DeCSS", that unscrambles the CSS and enables users to watch DVD films on unlicensed players and to copy them in digital format. As a result, the movie files can be sent over the Internet like any other digital file. Johansen offered DeCSS free of charge on his web site. From there it was downloaded and numerous other web sites posted copies.

DeCSS in conjunction with other software enables anybody to make a digital copy of a CSS-encoded DVD. All pieces of software needed for the decoding can be downloaded from the Internet at no cost.

The first step in copying a CSS encoded file onto the hard drive of a non-compatible computer consists in "ripping" (*i.e.*, extracting and decoding) the original DVD (.vob) file. Thereafter, the .vob file can be compressed to a file format playable in most computer media players. Additional encoding formats might then be applied to the compressed file in order to achieve an even greater compression rate that facilitates Internet transfer because the file becomes much smaller. Though the quality of this end product is inferior to the original DVD, it is still satisfactory for watching the movie on a computer screen.

The Legal Implications of DeCSS

On 9 January 2002, *ØKOKRIM* (the Norwegian Economic Crime Unit) indicted Johansen for breaking into another person's locked property to gain access to data that one is not entitled to access.[28] If convicted, Johansen could face a maximum prison term of two years, according to the Norwegian Criminal Code.[29] The claim is based on Section 145 that reads in its relevant part:[30]

"2. The same penalty shall apply to any person who by breaking a protective device or in a similar way unlawfully obtains access to data or software which are stored or transferred by electronic or other technical means."

The indictment responds positively to the claim of the DVDCCA and the Motion Picture Association.[31] The following issues will be crucial to the outcome of the case and all of them lack precedent under Norwegian law. First, whether the notion of "data" would encompass the CSS code – and not just movie files? Second, whether the breaking of the code to access material embedded in a disc that is owned by the person bypassing the protective device is covered by the provision? Third whether reverse engineering satisfies the requirements of criminal behaviour? Fourth, whether the right to reverse engineer, explicitly granted under Norwegian Law, can be waived by contract and in particular if the relevant contractual obligation is incurred as part of a licensing agreement executed over the Internet (see *infra* the description of the California Case)?[32]

The trial has still to be scheduled before any of these questions can be addressed.

In the United States, DVDCCA filed several lawsuits against the posting of, and linking to, web sites containing DeCSS. Meanwhile some of the cases have been settled. Others resulted in preliminary or permanent injunctions.

On 20 January 2000, a California trial court entered a preliminary injunction against Andrew Bunner to prevent him from any future disclosures of DeCSS by republishing on his web site or elsewhere the CSS unscrambling software. The court did not, however, ban the linking to other DeCSS posting web sites.[33] On 1 November 2001, the injunction was reversed on appeal.[34] As reported on 22 February 2002, the California Supreme Court will now hear the case.[35]

On 23 August 2000, the United States District Court for the Southern District of New York banned the posting of DeCSS on the Defendants' web site and enjoined them from knowingly linking their web site to any other web site displaying DeCSS.[36] Two of the Defendants, Eric Corley and his company 2600 Enterprises, Inc., appealed but on 28 November 2001, lost their case in the United States Court of Appeals for the Second Circuit.[37]

While the California lawsuit centres on provisions of the Californian version of the Uniform Trade Secrets Act, the New York claim focuses on a Federal Statute, namely the DMCA. Both cases meet in discussing the (US) Constitutional dimension of the creation, use and making available of DeCSS. Neither of these cases was directed against Johansen, but still his acts had to be evaluated implicitly.

The California Case (DVDCCA v. Bunner)

In Bunner, DVDCCA put forward the argument that DeCSS embodies, uses, and/or is a substantial derivation of its confidential proprietary information. Allegedly DeCSS contains the master key of an approved CSS licensee. This licensee offers CSS software exclusively under a license agreement prohibiting reverse engineering. Any user going through the software installment process consents to the agreement because during installation the End-User License Agreement appears on the screen stating that the "product in source code form" [38] is "confidential", a "trade secret" and the user "may not attempt to reverse engineer…any portion of the product."

Evaluating these facts, the trial court concluded that DVDCCA could claim CSS was a trade secret and that they had exerted reasonable efforts for its protection. It found that reverse engineering had unlocked this secret. Under the Californian Uniform Trade Secrets Act (Civil Code Section § 3426 – 3426.11),[39] a person who discloses or uses a trade secret of which he knew or should have known that another person obtained it by "improper means" or in violation of a nondisclosure obligation misappropriates that trade secret. The trial court assumed that Bunner disclosed DeCSS when he at least should have known that DeCSS had been created through the unauthorised use of proprietary CSS information that had been obtained by Johansen's illegally breaking the code. The illegality of Johansen's act resulted, however, from having violated the licence agreement that prohibited reverse engineering and not from reverse engineering itself because the latter is expressly excluded from being an improper means (Civil Code, § 3426.1 subd. (a)).

The trial court refrained from prohibiting links to other web sites, deciding that a web site owner was not liable for the content of other web sites. Moreover, the links were viewed as indispensable to Internet access.

The main aspect left for review by the Californian Court of Appeals was the trial court's evaluation of the First Amendment issue. It will be discussed *infra* together with the aspects added by the New York case.

The New York Case (DVDCCA v. Corley)

Corley focused on the question of whether DeCSS is an illicit circumvention tool under the DMCA. The DMCA transposes into US law *inter alia* the obligation of Article 11 of the WIPO Copyright Treaty (WCT) and Article 18 of the WIPO Performances and Phonograms Treaty (WPPT) to provide adequate and effective protection against the circumvention of technological measures used by copyright owners to protect their work. It thereby distinguishes between technological measures (i) that prevent unauthorised "access" to a copyrighted work (§ 1201 (a)(2)) and (ii) that prevent unauthorised "copying" of a copyrighted work (§ 1201 (b)(1)).[40] While trafficking is prohibited for both categories, the act of circumvention itself is forbidden only for the first.[41]

The District Court categorised CSS as an access controlling measure (§ 1201 (a)(2)) because the software requires various keys before it allows reading a CSS-protected work on a DVD. Access to those keys is granted exclusively by licensing agreement or via the purchase of a DVD player or drive containing the keys pursuant to such a licence. By developing DeCSS, Johansen circumvented this technological measure because DeCSS descrambles a scrambled work, the protected movie file, without the authority of the copyright owner (§ 1201 (a)(1)(A)).[42]

The District Court considered next whether Johansen could have successfully invoked what became known as the Linux defence. The Defendants alleged that Johansen created DeCSS solely to enhance the development of a DVD player that would run under the Linux operating system (which at the time did not exist). § 1201 (f) DMCA exempts from liability individuals who develop or use circumvention technology exclusively in order to identify and analyse elements of the programme necessary to achieve interoperability of computer programmes through reverse-engineering, provided that they are entitled to use a copy of the computer program for this purpose. DeCSS was concededly developed on and runs under Windows, so the decrypted files could obviously be copied like any other unprotected file using Linux or Windows. Furthermore, the District Court held that for Johansen the cracking of CSS had been an end in itself and a means of demonstrating his talent. At the utmost, the development of a Linux-based DVD player might have been among his goals. In any event for the Defendants, who had not authored DeCSS, the intention to foster Linux application would have been immaterial because, in principle, only a person who acquired information through reverse engineering may make that information available.

The District Court went on to judge the Defendants posting DeCSS on their web sites as violating the "anti-trafficking provisions" of both § 1201 (a)(2) and § 1201 (b)(1). While it thus focused mainly on the "access" alternative, the Appellate Court gave particular consideration to the technical question whether the CSS technique would also prevent unauthorised copying. It concluded that "the record leaves largely unclear how CSS protects against the copying of a DVD, as contrasted with the playing of a DVD on an unlicensed player" but that "the DeCSS program sidesteps whatever it is that blocks copying of the file". As a consequence, the anti-trafficking provision attaching to protection against illicit copying also applied.

For the access and the copying alternative, the law prohibits trafficking with devices that (i) are primarily designed or produced to circumvent; (ii) have only a limited commercially significant purpose or use other than to circumvent; or (iii) are marketed for use in circumventing.[43] The District Court affirmed all three alternatives because the offering or provision of the programme is the prohibited conduct – and it is prohibited irrespective of why the programme was written unless a statutory exception applies.

Then the District Court examined whether the DMCA violates the Copyright Act if it were to be interpreted as "eliminating" the fair use exemption codified in Section 107 of the Copyright Act. Indeed the CSS (protected by the DMCA) renders impossible some uses that might qualify for the exemption, particularly because it prevents exact copying of the whole or even parts of the digital file. According to the District Court, fair use is a defence to copyright infringement (and as such expressly left unaffected according to § 1201 (c)(1) DMCA) while the DMCA bans offering and providing technology designed to circumvent technological measures that control access to copyright works. Moreover, the DMCA prohibits only the act of circumvention and not the copying once authorised access has been obtained. In addition, it puts in concrete terms six exceptions that cover the fair use idea, among them reverse engineering, encryption research, and security testing.[44] The legislative history of the DMCA shows that Congress drew up this list in order to balance the conflicting interests and that it deliberately abstained from including a further reaching "fair use" defence.

The US Appellate Court confirmed these findings, adding that the US Supreme Court never found fair use to be constitutionally required.[45] Moreover, the Defendants had neither claimed fair use, nor was their fair use excluded by the injunction. In principal, copying CSS-protected material (e.g. by using a video camera) remained possible especially because fair use did not guarantee copying by the optimum method or in the identical format of the original.

The District Court also had to evaluate the linking to other web sites containing DeCSS. It considered whether this qualified as offering DeCSS to the public or as providing or otherwise trafficking in it within the meaning of § 1201 (a)(2) DMCA. It concluded: "the anti-trafficking provision of the DMCA is implicated where one presents, holds out or makes a circumvention technology or device available, knowing its nature, for the purpose of allowing others to acquire it." Applying this definition to the different types of linking, the Court took the following staggered approach: if sites linked to automatically start the process of downloading DeCSS, the linking equals transferring the DeCSS code to the user. This also applies where the hyperlink leads to a web page that basically gives only the choice of downloading. Only if the link goes to a page that offers "a good deal of content other than DeCSS" in addition to a hyperlink for downloading, or to a page for downloading, the case becomes arguable. Because the last alternative had not been invoked, the Defendants' linking violated the DMCA. The US Appellate Court confirmed this result.

Constitutional Dimension

The activities of Bunner and Corley were also examined with regard to their alleged constitutional dimension. In principle, both appellate courts agreed that DeCSS itself benefited from protection under the First Amendment. They diverged, however, on the questions of how much protection was required, and related thereto, whether or not free speech protection would cover the linking to other web sites offering DeCSS.

In a first and central step, the appellate courts had to determine whether the injunctions based on the DMCA and the Uniform Trade Secrets Act respectively, unconstitutionally imposed limits on "expressing" DeCSS? In principle, a statute may impose some restrictions on free speech but only subject to certain conditions. These are defined by the kind of speech in question and the level of scrutiny applied to judge the goals and means of the restriction.

Both appellate courts found that DeCSS is speech because it conveys information, namely the software code. The California Court of Appeals even expressly stated that it makes no difference that the defendant is a republisher rather than the original author of DeCSS. Further, the courts agree that DeCSS also contains a "functional" non-speech element. From here on, however, the views and reasoning of the two courts diverge.

The Californian Court of Appeals narrowed the speech element to capture only the "source code" which it labels as the preferred language for communication among programmers and as such "pure speech". It hints that the other function of the source code, namely to create object codes, lacks this quality because it does not generate ideas. Nevertheless and despite the questionable social value of DeCSS, it concluded that enjoining Bunner from disclosing DeCSS in source code format is prohibiting pure speech.

The Californian Court of Appeals also refused to apply precedents that upheld injunctions against trade secret misappropriations because in those cases voluntary agreements not to disclose a trade secret had waived the First Amendment protection. In contrast, in Bunner the statute itself and not a contractual nondisclosure obligation was used to overrule the constitutional protection. Precedents under copyright law may not be invoked either, because the Uniform Trade Secrets Act lacks the constitutional basis of the Copyright Act.

The Californian Court of Appeals concluded that the prohibition on disclosing the DeCSS source code constitutes prior restraint of pure speech as it kicks in before the communication occurs. It stressed state and federal jurisprudence that highly disfavour prior restraints and proscribe them with presumed unconstitutionality. Only if the protected interest would be more fundamental than the First Amendment itself could a prior restraint be upheld. According to the Californian Appellate Court this had never been the case and was not the case in Bunner.

By contrast, the US Appellate Court views DeCSS as mixed speech with the functional element being the consequence of its use, irrespective of whether DeCSS is displayed in source or object code. It points out that a simple mouse click launches the mechanism of DeCSS, which automatically decodes a scrambled video file. It finds that the provisions of the DMCA, on which the prohibition on DeCSS use and dissemination are based, targets the content-neutral, the non-speech, element. They serve a purpose that is unrelated to the content of expression, even though they might have an incidental effect on some speakers or messages.

The scrutiny test applied to content-neutral regulation is that it (i) has to pursue a substantial government interest, (ii) be unrelated to suppression of freedom of information, and (iii) be narrowly tailored in that it must not burden substantially more speech than is necessary to further that interest.[46] The US Appellate Court affirmed that preventing unauthorised access to encrypted copyrighted material is a substantial interest served by the prohibition. As an aside it remarked that Congress could regulate security devices for goods and that in the case of CSS only the form of communication but not the goal of regulation was different. It also confirmed compliance with the third and second prong of the scrutiny test. In particular, the District Court had not been required to employ the least restrictive means but only to avoid impairing substantially more speech than necessary. An interesting footnote (number 29) of the decision suggests that the latter point might have to be re-evaluated should future technology bring forth devices that allow single but prohibit serial copying.

The US Appellate Court agreed with the District Court that hyperlinking is also speech, underlining its mixed speech nature. A hyperlink conveys the Internet address of the linked web site (*i.e.*, information) and at the same time serves to actually connect the user's computer screen to this address (*i.e.*, functional aspect). The DMCA also passed the test for content-neutral regulation to the extent that it authorises the ban of hyperlinking.

The US Appellate Court acknowledged possible impairments to free expression through the linking prohibition. For example, web site operators fearing that another web site could display DeCSS might not hyperlink to that web site with the result that other information of that website becomes inaccessible. Nevertheless, the Court found that the narrow tailoring requirement of the scrutiny test was satisfied. Particularly, it rejected the requirement of intent to cause harm or of applying the elements that allow enjoining print media. Further, it did not embrace the heightened standard proposed by the District Court. Instead it concluded that some choice had to be made between impairing some communication and tolerating decryption, but that this decision was one of public policy to be left to Congress. Congress, however, by passing the DMCA, had voted for protecting encryption.

Conclusion

The case law concerning peer-to-peer systems illustrates: innovation of software and technology used to exchange digital files over the Internet relates to legal concepts targeting copyright piracy. Software developers tried to bring the online exchange of audio and audio-visual files beyond legal scrutiny by designing systems such as Napster and Grokster. The audio-visual industry striving to regain control over copyrighted works battled back by creating CSS to supplement allegedly incomplete legal protection. The answer of the software programmers followed promptly with the authoring of DeCSS and armistice is not on the horizon. As a result additional parties (the creators of CSS and DeCSS) have fuelled the litigation surrounding movies online.

New legal instruments were injected as well. WIPO contracting parties entered the commitment to strengthen the legal position of copyright owners by warranting adequate protection for technological measures. The pertinent provisions of the DMCA have already been discussed. The European counterpart, Chapter III of the Directive, obliges Member States to provide adequate legal protection against the circumvention of technological measures and the manufacturing or trafficking with such circumvention tools (Art. 6). The objective and subjective elements to be covered by national legislation correspond largely to those stipulated by the US law, which gives ample reason to closely monitor the DeCSS litigation.

Yet were the DeCSS litigation to take place in Europe, it would have its own very specific traits. This is inevitable because the WIPO instruments had to consolidate the interests of all contracting parties and therefore are phrased in very general terms. In addition, the Directive itself attempts to harmonise national laws. This is particularly notable with regard to Art. 6 para. 4, addressing seven limitations to copyrights that if granted by a Member State must remain accessible for the beneficiaries. [47] Different from the DMCA, this mandatory rule applies exclusively to the act of circumvention and leaves the protection against trafficking with access or control devices intact.[48] The Directive leaves it to the discretion of national legislators to allow some form of private use. In contrast, in the United States the further determination of fair use lies with the courts.

The private/fair use exception is probably the most significant tool in balancing the interests underlying the present litigation: that is those of the copyright holder and those of the public in some forms of copyright exempted use. The public interest is particularly important where it borders on freedom of speech/expression – an acknowledged pillar of democracy. Koelman has argued that "copyright constitutes a form of information policy, serving the public interest in maximizing the availability of information products by, on the one hand, granting an exclusive right and thereby providing for an incentive to create and by, on the other hand, limiting the scope of the monopoly copyright provides for to ensure information will be widely available and usable." He then concludes that "technological protection measures expand the control of rights holders and potentially upset the balance".[49] Yet according to rightsholders imbalance had already been caused by the unauthorised copying of audio-visual works.

The struggle for the "right" balance continues. In the United States, the Consumer Broadband and Digital Television Act of 2002 has just been introduced in the US Senate. The law will oblige the industry to agree on a copy-protection system to be embedded in all digital media devices (both hardware and software).[50] The system shall hinder unauthorised copying while allowing legitimate uses. Whereas the law has still to be adopted, the ultimate test of its success is already carved in stone. It is simply whether the law can render the next generation of circumvention devices superfluous.

1) For example, worldwide replication of DVD-Videos increased from 194 million copies in the year 1999 to 474 million in 2000 to 905 million in 2001. See Statistical Yearbook 2001 of the European Audiovisual Observatory at page 125.
2) Susanne Nikoltchev & Francisco Javier Cabrera Blázquez, "MP3: Fair or Unfair Use", in IRIS Focus: Copyright Law in the Digital Age, available at http://www.obs.coe.int/oea_publ/iris/iris_plus/focus8_2000
3) MP3 is an audio compression file format for digital sound recordings.
4) A recent example of this was Movie88.com, a web site offering via streaming a full range of copyrighted films at a rate of USD 1 for a three-day viewing-period. In the meanwhile the Internet Service Provider has closed its web site.
5) The Gnutella system is described in the MP3 article, under E.
6) The recording industry has only recently released copy-protected CDs. These CDs would play on (most) standard CD players, but not on computer CD ROMs.
7) For examples, see the MP3 article, under A. and B.
8) UMG Recordings, Inc. et al. v. MP3.Com, Inc, Case 00 Civ. 0472 (S.D.N.Y. 2000). An unofficial version of the Ruling of 6 September 2000 is available at: http://news.findlaw.com/cnn/docs/mp3/0906_mp3_unoffruling.html
9) A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001), dated 12 February 2001, available at:
http://www.ce9.uscourts.gov/web/newopinions.nsf/4bc2cbe0ce5be94e88256927007a37b9/c4f204f69c2538f6882569f100616b06?OpenDocument
For a summary of the decision see IRIS 2001-4: 13.
10) In Napster, the Appeals Court held that Napster users uploading and downloading files violated the distribution right and the reproduction right respectively (17 U.S.C. § 106 (1) respectively (3)).
11) Court of First Instance of Antwerp, Case IFPI Belgium v. Werner Guido Beckers (ARK no. 99/594/C), Order of 21 December 1999.
12) See Napster Case, *ibid*, at VII. C. In the preliminary proceedings, this defence of copyright misuse was rejected because it is not valid against injunctive relief. Meanwhile the District Court ordered further discovery to determine whether plaintiffs have misused their copyrights in order to monopolise the digital distribution market. The Order, dated 21 February 2002, is available at
http://www.cand.uscourts.gov/cand/tentrule.nsf/4f9d4c4a03b0cf70882567980073b2e4/31e0b537993cd73288256b6800673c73?OpenDocument
13) See the historical discourse with further references by Hermann Cohen Jehoram, *Einige Grundsätze zu den Ausnahmen im Urheberrecht*, in GRUR Int 2001, p. 807.
14) European Parliament and Council Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, OJ L 167 of 22 June 2001, p.10-19.
http://europa.eu.int/cgi-bin/eur-lex/udl.pl?REQUEST=Seek-Deliver&COLLECTION=oj&SERVICE=eurlex&LANGUAGE=en&DOCID=2001l167p0010
15) For the legislative history and a detailed description of Art. 5 see Jörg Rheinbothe, *Die EG-Richtlinie zum Urheberrecht in der Informationsgesellschaft*, GRUR Int 2001, p. 733 (739-740).
16) Rheinbothe, *ibid*, p. 739.
17) These two doctrines are discussed *infra* for MGM v. Grokster.
18) Pub.L.No. 105-304, 112 Stat. 2860 (1998).
19) See Consideration 25 of the Directive.
20) United States District Court Central District of California, Western Division Metro-Goldwyn-Mayer Studios Inc., et al. v. Grokster, Ltd., et al., Case No. CV 01-08541 Svw (Rnbx). All court documents concerning this case can be found at: http://www.eff.org/IP/P2P/MGM_v_Grokster/
21) On 4 March, the U.S. District Court dismissed the Defendant's motion for partial summary judgement as premature. The transcription of the hearing is available at:
http://www.eff.org/IP/P2P/MGM_v_Grokster/20020304_mgm_hearing_transcript.html. In an unrelated case, the District Court of Amsterdam on 29 November 2001 ordered Kazaa to take measures to stop the infringement of copyright through unauthorised music files on their network. See IRIS 2002-1: 13. On 28 March 2002, this ruling was overturned on appeal.
See http://story.news.yahoo.com/news?tmpl=story&cid=581&u=/nm/20020328/tc_nm/tech_entertainment_dc_2
22) On 4 March 2002, this complaint was consolidated with a similar complaint filed by songwriters and music publishers against the same defendants. All court documents relating to the latter are available at: http://www.eff.org/IP/P2P/NMPA_v_MusicCity/
23) See Gershwin Publ'g Corp. v. Columbia Artists Mgmt., Inc., 443 F.2d 1159, 1162 (2d Cir. 1971).
24) Sony Corporation of America v. Universal City Studios, Inc., 464 U.S. 417, 104 S. Ct . 774, 78 L. Ed. 2d 574 (1984), dated 17 January 1984, available at:
http://www.eff.org/Legal/Cases/sony_v_universal_decision.html
25) See Gershwin Publ'g Corp. v. Columbia Artists Mgmt., Inc.
26) There the Court of Appeals quotes Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259 (9th Cir. 1996) available at:
http://www.law.cornell.edu/copyright/cases/76_F3d_259.htm
27) Fred von Lohmann, "Sharing and Copyright Law after Napster", available at: http://www.eff.org/IP/P2P/Napster/20010227_p2p_copyright_white_paper.html
28) For more information see http://www.eff.org/IP/Video/DeCSS_prosecutions/Johansen_DeCSS_case/20020110_eff_pr.html
29) Law of 22 May 1902 no. 10, amended by laws of 16 February 1979 no. 3 and of 12 June 1987 no. 54.
30) For this translation and the original version see the Declaration of Jon Bing of 18 January 2000 at
http://www.eff.org/IP/Video/DVDCCA_case/20000118_bing_norway_law_decl.html
31) See the English translation of their attorney's letter to ØKOKRIM at http://www.eff.org/IP/DeCSS_prosecutions/Johansen_DeCSS_case/20000104_dvdcca_no_prosecutor_letter.en.html
32) See Declaration of Jon Bing for further details of the upcoming legal questions; endnote 30.
33) Santa Clara County Superior Court, Order Granting Preliminary Injunction for the plaintiffs against the defendants, in DVDCCA v. McLaughlin, Bunner et al., available at:
http://www.eff.org/IP/Video/DVDCCA_case/20000120-pi-order.html
34) Court of Appeal of the State of California Sixth Appellate District, overturning DeCSS injunction in DVDCCA v. Bunner, available at http://www.eff.org/IP/Video/DVDCCA_case/20011101_bunner_appellate_decision.pdf
35) See Newsbytes.com at
http://www.newsbytes.com/news/02/174688.html
36) Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 346 (S.D.N.Y. 2000).
37) United States Court of Appeals for the Second Circuit, Docket No. 00-9185.
Universal City Studios, Inc. v. Reimerdes
38) Source Code is the text of a computer programme written in a programming language. To be understood by the computer, this code has to be translated into machine "readable" strings of 1's and 0's, called the Object Code.
39) The Act is available at http://www.leginfo.ca.gov/cgi-bin/display-code?section=civ&group=03001-04000&file=3426-3426.11
40) See US Copyright Office Summary, The Digital Millennium Copyright Act of 1998, December 1998 at page 4 et seq.
41) See § 1201 (a)(1)(A).
42) For the definition of circumvention see (§ 1201 (a)(3)).
43) See § 1201 (a)(2) and § 1201 (b)(1).
44) The Court denied that posting of DeCSS could be viewed and thus justified as encryption research or security testing. For the other exceptions see § 1201 (d) to (j).
45) In contrast, the California Appellate Court, though actually not concerned with copyrights but with trade secrets, stressed that the fair use doctrine has served to uphold injunctions in copyright infringement cases with a view to its First Amendment implications and, in this context, that Art. I, § 8 cl. 8 of the US Constitution confers constitutional authority upon the Copyright Act.
46) Turner Broadcasting System, Inc. v. FCC, 512 U.S. 622, 662 (1994) quoting Ward v. Rock Against Racism, 491 U.S. 781, 799 (1989).
47) These exceptions are reprographies, public institutions and archives, ephemeral recordings, non-commercial social institutions, teaching and research, use by disabled persons, and public security/proceedings
48) The DMCA exceptions apply according to the distinction of "access" or "copy" control. Most of them also apply to the anti-trafficking prohibition. For details, see § 1201 (d) to (j) DMCA.
49) See Kamiel J. Koelman, "A hard Nut to Crack: The Protection of Technological Measures", EIPR 2000, pp 272-280 (279)
50) The draft is available at
http://www.politechbot.com/docs/cbdtpa/hollings.s2048.032102.html