A Brief Primer on U. S. Copyright Protection for Works on the Internet

By Professor Doris Estelle Long*

With an estimated 934 million users globally, the Internet poses an enormous opportunity for small and medium enterprises to become full, active members in the burgeoning global, digital marketplace. Yet in order for the opportunities afforded by the growth of electronic commerce (e-commerce) to be fully enjoyed, countries must establish appropriate legal regimes and enforcement methodologies to protect the content which drives electronic commerce. Rapid advances in technology have lowered entry barriers and made it easier for more businesses to participate on the global marketplace. Yet these same advances have also made it easier for pirates and counterfeiters to use the Internet to distribute their own illegal products.

This primer is intended to be a brief review of some of the more significant legal developments in the United States dealing with the unique problems posed in protecting intellectual property on the Internet. As a result of the rapid growth of the Internet, and the advances in such new communication techniques as peer to peer communication, law in the United States is changing on an accelerated basis to meet the challenges posed by these rapid advances. Because of the special issues posed by the Internet, the United States has developed new theories and new statutes for the protection of intellectual property on the Internet. Among the new statutes which will be discussed in this primer is the Digital Millennium Copyright Act.

This primer should be considered as merely a snapshot view of present US protection trends in the area. It is intended to discuss some of the most important developments in the law, but is *not* intended to be a comprehensive discussion of all the issues and cases in the area. It is also *not* intended to take the place of consultation with qualified lawyers regarding the application of US law to any particular action or situation.

The Challenge of Technology

The rapid development of the Internet, combined with the widespread availability of personal computers, and advances in software and other technology that supports the Internet, have created new opportunities for intellectual property owners on a global basis. These new opportunities include new methods for advertising products and services, and for their distribution (including digitally) to far flung customers. The rapid reproduction and distribution

* Professor of Law, The John Marshall Law School, Chicago, ILL, USA 60604.

of IP-protected works permitted by such technological advances, however, has also helped to fuel an increasing global piracy problem. Thus, the Internet poses unparalleled opportunities for commercial growth and global communication. However, it also poses unparalleled opportunities for abuse by pirates, counterfeiters and other free riders.

The Exponential Growth of Internet Piracy

The truth is no one can accurately measure the scope of piracy on the Internet. The International Intellectual Property Alliance contends that global piracy, exclusive of Internet piracy, resulted in losses of over $ 84 billion dollars in 2001. Internet piracy is estimated to exceed these amounts, but is largely incapable of accurate measurement because it is so ubiquitous and clandestine. There is no doubt, however, that the problem is increasing, both in scope and frequency. As technology advances, so apparently does piracy. No category of work is safe. Movies, songs, poems, books, photography, software, quilting patterns, novels … anything that can be digitally reproduced can be pirated.

Countless factors have contributed to this increasing problem. Perhaps the most significant contributing factors to the growth in global digital piracy is the simple ease of reproduction offered by modern reproductive technologies. Not only can digital copies be created at ever-diminishing costs, these copies, unlike the analog copies of old, are virtually indistinguishable from the original in quality. Worse, the creation of such copies generally does not diminish the quality of the original. Consequently, engaging in peer-to-peer file sharing, and providing potentially hundreds of copies of a favorite digital song to strangers, does not adversely affect the ability of the helpful pirate to continue to enjoy that song. Unlike the old days, a helpful pirate does not even have to relinquish physical possession of his favorite CD (however temporarily) for others to copy the songs they desire. With modern technology, one can literally have one's song and pirate it too with no inconvenience whatsoever.

Digital piracy is also relatively inexpensive. With the growth of Internet cafes globally, would-be pirates no longer need to invest in expensive computers or duplicating machines. Money to pay for Internet access fees, and one disc of recordable memory is sufficient.

Digital piracy has become push-button easy. Some computer programs, such as Gnutella, seem to require a certain level of technical expertise (or patience) before they can be successfully downloaded and used in peer-to-peer pirate distribution networks. Countless others, such as the now-largely dismantled Napster, however, are almost idiot-proof. Transfer technology that allows people to copy ("burn") music from one CD to another is so simple, a child can do it. And reproduction times continually drop as compression technology improves. Even the inconvenience of time has disappeared.

Further fueling global Internet piracy is an increasing "disconnect" in end users' minds and website owners' minds between physical theft and electronic theft. People who would never engage in shoplifting have no apparent compunction in making and distributing illegal downloads of copyrighted songs.

Unfortunately, although technology has created the "problem" of piracy," it has not created its solution. There is currently no foolproof copy code or encryption technique that has been developed to keep pirates from illegally copying songs from music CD's. To be honest, I seriously doubt that any such "foolproof" technology will ever be created. No matter how sophisticated the technique, somewhere in the world there is some computer hacker who will be able to circumvent the technology. But "foolproof" methods are not required. *Effective* methods capable of discouraging all but the hard-core pirate should be sufficient to substantially reduce global piracy (and would be a marked improvement over the current status quo).

US Copyright Law and the Internet

A General Introduction

Under US copyright law, copyright protection is extended to "original works of authorship fixed in any tangible medium of expression now known or later developed from which they can be perceived, reproduced or otherwise communicated…" (17 U.S.C. §102(a)) Copyright protection does not extend to "any idea, procedure, process, system, method of operation, concept, principle or discovery.' (17 U.S.C. §102(b)) In essence, so long as a work has been recorded, filmed, written or otherwise set out in a tangible form, it may be subject to protection under US copyright law. Consequently, literary, dramatic, musical, artistic or other intellectual works, including original collections of information may be protected. Thus, under US copyright law, such diverse works as computer software, paintings, choreography, maps, poetry and sound recordings may be protected so long as such works are "original" and contain "expression." Such protection applies to both published and unpublished works. Furthermore, no registration or notice on the work is required for the work to be protected. Instead, creation of the work alone is sufficient.

Upon the creation of a copyright protectable work the author (or copyright owner) is entitled to a bundle of six rights. These rights include the exclusive right to do or authorize the following acts:

- The right to reproduce, in whole or in part, the work in copies;
- The right to prepare derivative works based upon the original;
- The right to distribute copies of the work to the public;

- The right to perform the work publicly;
- The right to display the work publicly;
- In the case of sound recordings, the right to perform the work publicly by means of a digital audio transmission.

While copyright registration is not required for protection, US authors are required to register their works before seeking legal relief for infringement. . Copyright registration is controlled by the US Copyright Office and can be done over the Internet. Moreover, where litigation is imminent, registration may be obtained on a expedited basis. In order to prove copyright infringement, a plaintiff must prove the following:

- That he is the copyright owner;
- That the work is copyright protected; and
- That the copyright in the work has been infringed.

For example, if the claim is that the work has been reproduced without authorization, then the copyright owner must demonstrate that the work has been copied without permission. Such copying does not have to be verbatim to qualify as infringement. Instead, it is sufficient if an ordinary observer would consider the expressive elements "substantially similar."

US copyright law provides for a complete panoply of remedies for copyright infringement, including injunctive relief, seizure and destruction of the infringing copies as well as all plates, molds, matrices, masters, tapes, film negatives, or other articles by means of which infringing copies or phonorecords may be created, actual damages (including lost profits), statutory damages, up to $150,000 per infringement for willful infringement, costs and reasonable attorneys' fees. The parties that may be held liable for copyright infringement include the party which committed the infringing act (referred to as a "direct infringer"), the party which knew, or had reason to know, of the infringing activity and induces, causes or materially contributes to it (referred to as a "contributory infringer") and the party which has the right and ability to supervise the parties engaged in the infringing activities and who had a direct financial interest in the exploitation of the copyrighted material (referred to as "vicarious liability").

No Electronic Theft ("NET") Act

US law also provides criminal penalties for copyright piracy, including monetary fines and penalties, and imprisonment. (17 USC §506(a)). *See also* 18 USC § 2319) No commercial advantage or private financial gain is required for criminal penalties to attach in the United States. Evidence of such motivation is an enhancing factor which increases the minimum sanctions that may be imposed.

There are four essential elements to a charge of criminal copyright infringement under 17 USC § 506(a). The government must demonstrate: (1) that a valid copyright; (2) was infringed by the defendant; (3) willfully; and (4) that a certain threshold amount of goods were sold or offered for illegal distribution (required for certain felony convictions). The threshold limits for felony convictions require that the defendant reproduced and/or distributed at least 10 copies of one or more copyrighted works with a total retail value of more than $2,500 within a single 180-day period. Misdemeanor convictions are available if the infringement was done *either* for purposes of commercial advantage or private financial gain (in which case no threshold amount applies), or by reproduction or distribution of one or more copyrighted works with a total retail value of more than $1,000 within a 180-day period. In the latter case, no commercial motivation is required.

Fair Use

One of the most significant defenses to a claim of copyright infringement is the defense of "fair use." This doctrine is codified in Section 107 of the 1976 "Act which provides that the "fair use of a copyrighted work… for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship or research is not an infringement of copyright." These uses are not categorical fair uses, but instead are simply examples of the types of uses which might be considered fair. To determine whether an unauthorized use of a copyrighted work qualifies as a fair use, courts consider the following four statutory factors. They are:

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

(17 U.S.C. §107) These factors are not exclusive. Instead, courts often consider additional factors, including whether the use in question is protected under the First Amendment's free speech protections, or whether it qualifies as a "transformative" use of the original work.

The Digital Millenium Copyright Act (DMCA)

As noted above, one of the major hurdles US Copyright law has faced in recent history is the dawn of the Internet. The Internet allows for works to be displayed quicker and for copies to be created at a faster pace then ever before

and with a higher degree to authenticity. Because of the nature of the Internet, the party which is directly involved in the infringing activity may be an end user. Thus for example, many acts of copyright infringement occur as a result of the unauthorized "uploading" (reproducing onto a web site) of a copyrighted work without the authorization of the copyright owner. While end users may be directly responsible for the infringing activity, their infringing activity most likely would not occur without the help of the Bulletin Board or Internet Service Provider. Thus, one of the early issues which the United States faced in dealing with copyright infringement on the Internet was the extent to which service providers would be responsible for the infringing acts of their end users.

Early case law provided that, in certain circumstances, bulletin board and Internet service providers might be liable if they gained some type of financial benefit from the unauthorized activities of their end users. Thus, for example, in *Playboy Enterprises, Inc. v. Frena,* 839 F. Supp. 1552 (M.D. Fla. 1993), the court found that the operator of a computer bulletin board was directly liable for copyright infringement when unknown subscribers had both uploaded and downloaded copyrighted photographs from the plaintiff's magazine without permission.

By contrast, however, in *Religious Technology Center v. Netcom On-Line Communications Services, Inc.,* 907 F. Supp. 1361 (N.D. Cal. 1995), the court declined to find the operator of a computer bulletin board directly liable for the unauthorized uploading and downloading of copyrighted materials by its subscribers. The plaintiff's organization held the copyright to certain publications which were published by the defendants. The court was not persuaded by the plaintiff's argument that an individual who stores copied material or makes the copyrighted material available is also guilty of direct copyright infringement, particularly where the service provider did not charge an access fee. The court, however, left the issue of contributory infringement open.

Internet Service Provider Liability

Ultimately, Congress addressed the question of service provider liability in the Digital Millennium Copyright Act, or DMCA, enacted in 1998. Significantly, the statute provided a safe harbor for certain specified activities by service providers. Section 512 of the Act, referred to as the "safe harbor" provision of the statute releases a service provider from liability if it (1) qualifies as a service provider within the meaning of the statute; (2) adopts and reasonably implements a policy of terminating in appropriate circumstances the accounts of subscribers who are repeat infringers; (3) accommodates and does not interfere with "standard technical measures" copyright owners use to identify or protect copyrighted works; and (4) meets other specified requirements regarding the particular activity in question (see below). The four activities for which safe harbor protections are available are:

- Serving as a conduit for transitory communications;
- System caching;
- Posting information at the direction of end users;
- Hyperlinks and other information location tools.

Transitory Communications

Section 512(a) of the DMCA provides a safe harbor for ISP's who act as conduits for transitory communications. To qualify as a transitory communication, the transmission be initiated by a person other than the ISP. The transmission must be carried out through an automatic technical process The ISP must not select the recipients of the material, or directly copy the material in question, or alter the transmitted material and must maintain a temporary copy of the material for no longer than reasonably necessary. Moreover, this temporary copy may not be accessible to third parties. Examples of transitory or conduit activities are ISP's which provide email access or file sharing access to the Internet.

System Caching

Section 512(b) of the DMCA provides a safe harbor for ISP's who maintain system caches of materials for a limited time to allow the materials to be provided to subscribers who have requested the material previously without the need to retrieve such materials from the system. To qualify for a safe harbor, the material must be available on line by someone other than the ISP. The material must be transmitted without modification; and temporary storage must be carried out through an automatic technical process. The provider must not interfere with technology that returns "hit" information to the person who posted the material and the provider must limit users' access to the material in accordance with conditions on access (e.g., password protection) imposed by the person who posted the material. In addition, any material that is posted without the copyright owner's authorization must be promptly blocked or removed once notice has been received regarding the infringement. (See discussion below regarding "notice and takedown provisions")

User Postings and Storage

Section 512(c) of the DMCA limits the liability of service providers for posting infringing material on websites (or other information repositories) hosted on their systems. It applies to only to postings and storage at the direction of a user. In order to be eligible for the limitation, the ISP must not have actual knowledge that the material is infringing and must not be aware of facts or circumstances from which such infringing activity is apparent. If the ISP has the ability to control the infringing activity, it must not receive a financial benefit which is directly attributable to the infringing activity. Upon receiving proper notification of claimed infringement, the ISP must expeditiously take down or block access

to the material. In addition, a service provider must have filed with the Copyright Office a designation of an agent to receive notifications of claimed infringement and must have posted agent contact information on its website..

Hyperlinks and Other Information Research Tools

Section 512(d) of the DMCA limits the liability of service providers for posting or providing hyperlinks, online directories, search engines and the like. In order to be eligible for the limitation, the ISP must not have actual knowledge that the material in question is infringing and must not be aware of facts or circumstances from which such infringing activity is apparent. If the ISP has the ability to control the infringing activity, it must not receive a financial benefit which is directly attributable to the infringing activity. Upon receiving proper notification of claimed infringement, the ISP must expeditiously take down or block access to the material. In addition, a service provider must have filed with the Copyright Office a designation of an agent to receive notifications of claimed infringement and must have posted agent contact information on its web site.

Other Exceptions

In addition to the "safe harbor" provisions listed above, the DMCA provides additional exceptions from liability for non-profit educational institutions, an allowance for technology development through reverse engineering means and encryption research, an exception for technology necessary to protect minors on the Internet, and technology necessary for testing of computer security. Each of these exceptions is narrowly tailored and has been the subject of harsh criticism by some scholars and user groups. Thus, for example, the encryption research exception has been limited to researchers who have been "authorized" by the copyright owner, or are otherwise engaged in non-amateur encryption research. By its language, it would appear to preclude amateur and other outside researchers from conducting (or at least sharing) studies of the efficacy of certain technological protection measures. Such a narrow exception has been criticized for its potential "chilling effect" on encryption research.

Notice and Takedown Provisions

As noted above, in order for an ISP to qualify for certain safe harbors, it must promptly remove infringing material, or prevent access to such materials, as soon as the ISP has notice of the infringing acts. Where copyright owners become aware of infringing materials, they must provide a written notice that includes an authorized signature (which may be an electronic one), a clear identification of the copyrighted work allegedly being infringed, a clear identification of the alleged infringing material, "reasonably sufficient" information that will allow the ISP to locate the material at issue, information, such as an email address, that will allow the ISP to contact the subject of the infringing

activity, a statement of good faith on the part of the copyright holder and a statement that the provided information is accurate. (17 U.S.C. §512(c)(3))

On receipt of a proper notice from a complaining copyright holder, the ISP must expeditiously remove the infringing material or block access to it. The ISP must also take reasonable steps to notify the subscriber that it has removed or disabled access to the material in question. Upon receipt from the subscriber of an appropriate counter notification in writing, containing a statement under penalty of perjury that the subscriber has a good faith belief that the material was removed or disabled "as a result of mistake or misidentification," the ISP must notify the complaining copyright holder of the counter notification and must inform the holder that it will replace the removed material or cease disabling access to it in 10 business days. (17 U.S.C. §512(g))

Where an ISP acts in good faith in response to a notice of infringement, it will not be liable so long as it replaces any removed material subject to a proper counter complaint within 10 to 14 days of receipt of the counter notice. If the ISP receives notice from the original complaining party that it has filed a lawsuit regarding the material in question such material does not have to be replaced until ordered by the court to do so. (17 U.S.C. §512(g))

Identity Subpoenas

Under Section 512(h), the DMCA grants copyright owners the ability to obtain a subpoena on request of a clerk of any United States District Court for disclosure by a service provider of the identity of a subscriber who has allegedly engaged in copyright infringement. (17 U.S.C. § 512(h)) To obtain the subpoena, the copyright owner is only required to provide a written notice that includes a clear identification of the copyrighted work allegedly being infringed, a clear identification of the alleged infringing material, "reasonably sufficient" information that will allow the ISP to locate the material at issue, a statement of good faith belief the work is being infringed and a declaration that the identity is being sought and will only be used for the purpose of protecting the owner's copyright. (17 U.S.C. §512(h)). Unlike the notice and take down provisions of Section 512(c), which requires Internet service providers who seek a safe harbor from copyright liability to remove infringing materials upon notice, there is no requirement that the subscribers whose identity is being sought be notified of the subpoena or given an opportunity to challenge its propriety prior to disclosure of their identity. Moreover, such subpoenas are issued as a ministerial act of the clerk of the court, without the need for judicial oversight.

In *Recording Industry Association of America, Inc. v. Verizon Internet Services, Inc.*, 351 F3d 1229 (D.C.Cir. 2003), the DC Circuit Court of Appeals held that the subpoena provisions of Section 512 (h) did *not* apply to Internet Service Providers who "solely act as a conduit for data transferred between two internet users, such as persons sending and receiving e-mail or, as in this case,

sharing P2P files." Relying on the statutory language of Section 512 (h), as well as its overall structure, the court held that subpoenas "may only be issued to an ISP engaged in storing on its servers material that is infringing or the subject of infringing activity." While ISP's who serve as web operators, or who provide caching or location services store materials on their servers, providers like Verizon who only provide transmission services, fall outside the scope of Section 512(h).

While the court's decision in *Verizon* removes conduit or transmission ISP's from the subpoena provisions of 512(h)(at least in the DC Circuit), it does not wholly remove the ability of copyright owners to discover the identity of end users who are engaged in illegal P2P file trading. Copyright owners may still obtain the necessary information from conduit ISP's by filing a "John Doe" complaint and then obtaining a subpoena requiring the ISP to disclose the end user's identity. If the court's decision in *Verizon* is widely adopted, and the statute is not thereafter changed, however, the cost of end user litigation will increase as a result of the need to pursue the more costly "John Doe" subpoena process. These higher costs will ultimately be passed onto the defendants with the unfortunate result that the ability to settle disputes prior to the institution of a lawsuit may be severely curtailed.

Anti-Circumvention Devices

Under the Digital Millenium Copyright Act (DMCA) the making or selling of devices or services used to circumvent technological measures to prevent either unauthorized access or unauthorized copying of a copyrighted work is prohibited where such devices or services are *primarily* designed or produced to circumvent "technological protection measures." (17 U.S.C. §1201)

Section 1201 of the 1976 Copyright Act (amended) prohibits the circumvention of technological protection measures designed to control access to a copyrighted work (17 USC § 1201(a)). To qualify for protection the technological measure in question must be "effective." Effectiveness, however, does not mean that the measure must be perfect or nearly impossible to break. Instead, it is sufficient if the measure "actually works" when decryption programs or other circumvention measures are absent. (*See Universal City Studios, Inc. v. Reimerdes*,111 F. Supp.2d 294 (SDNY 2000), *aff'd on other grounds sub nom. Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir. 2001).)

In addition to prohibiting the actual circumvention of technological protection measures, the Act also prohibits the manufacture, importation, offering to the public, provision or other "trafficking" "in any technology, product, service, device, component or part that is *primarily designed* or produced for the purpose of circumventing a [protected] technological protection measure that either effectively controls access or protects a right of the copyright owner." (17 USC §§ 1201(a)(2) & (b)(1)(emphasis added))

Violations of these anti-circumvention provisions may be challenged by both civil and criminal actions. Successful civil litigants are entitled to the full panoply of remedies, including statutory damages of not less than $200 nor more than $2,500 "per act of circumvention, device, product, component, offer or performance of service." (17 USC § 1203) Criminal violations require proof of willfulness and motivation for commercial advantage or private financial gain. (17 USC § 1204) First time offenders may be subjected to penalties of up to $500,000 in fines and/or imprisonment for not more than 5 years. Recidivist penalties are significantly elevated. (*Id.)*

The statute provides for numerous categorical exceptions, including, limited circumvention rights for:

- Non-profit libraries, archives and educational institutions;
- Law enforcement, intelligence and other government activities;
- Reverse engineering;
- Encryption research;
- Security testing ; and
- Protecting personal identification information.

Under the exemption for a "non-profit library, archives, or educational institution", such institutions which gain access to a "commercially exploited copyrighted work "solely in order to make a good faith determination whether to acquire a copy of that work are exempt from liability so long as they keep the copy no longer than necessary to make a good faith determination and may not be used for any other reason. This exemption is inapplicable if an identical copy of the work is "not reasonably available in another form." The exemption is further limited since it only applies to acts of circumvention, and not to any trafficking in circumvention devices, etc. To qualify for this exemption, the library or archives in question must be open to the public or must be available to more than the researchers affiliated with it who are doing research in a specialized field.

Notably, the access and trafficking provisions of the DMCA do not provide a categorical exception for "fair use" activities unrelated to the above-specified categories. Thus, for example, a teacher who seeks to circumvent technological protection measures for the purpose of obtaining access to materials to use in teaching activities is not excused from compliance, even if the use of such materials might otherwise qualify as a fair use under traditional copyright principles.

This lack of a "generic" fair use defense for purported circumvention violations has created the greatest challenge to the continued viability of the anti-circumvention provisions of the DMCA. Present bills before Congress would add

such a generic exception to the Act. (*See, e.g.,* Benefit Authors without Limiting Advancement or Net Consumer Expectations (BALANCE) Act of 2003, HR 1066)

It should be noted that the provisions of the DMCA that provide limited protection from liability for copyright infringement by certain ISP's discussed above does *not* apply to claims regarding the trafficking, etc. of circumvention products and technologies. In addition, although reverse engineering is allowed under the statute, circumvention of existing technology is prohibited except in the limited circumstance of reverse engineering for the purpose of achieving interoperability.

One of the most recent cases which dealt with the scope of protection available under the DMCA for technological protection measures is *Universal City Studios, Inc. v. Corley,* 273 F.3d 429 (2d Cir. 2001). In this case the court dealt with the liability of Shawn Reimerdes, who ran a website that published decryption technology for DVD's. Most works placed on DVD's are protected by a copy protection technology called CSS which is designed to prevent the unauthorized copying of motion pictures in DVD format. Decryption technology, called DeCSS, circumvents the CSS-protected motion pictures on DVD's and allows end users to reproduce the motion pictures contained on such copy-protected discs. Reimerdes made this DeCSS available on the Internet through his website and by linking his website to the same information contained on other websites. Reimerdes was sued by eight major United States motion picture studios. In addition to dealing with the question of liability under the DMCA's anti-circumvention prohibitions, the court also had to face issues raised by the defendant's defense under the First Amendment (free speech). The court held that defendant had violated the DMCA and enjoined the defendant from both publishing the decryption information as well as linking its site to others that posted the DeCSS code. The court further rejected the defendant's free speech defense. The court recognized that computer code qualified as "speech" under the First Amendment. It held, however, that the anticircumvention provisions of the DMCA did not target the speech components of the code. Instead, they targeted the functional capabilities of the code to instruct a computer to decrypt CSS. Such functional capability was not speech. Even if it were, the court in dicta indicated that the anticircumvention provisions were still constitutional since they qualified as content neutral regulations that met the substantial governmental interest in preventing piracy.

Copyright Management Information

In addition to protecting technological protection measures, the DMCA also protected the integrity of copyright management information. Section 1202 of the 1976 Copyright Act (amended) prohibits the unauthorized, intentional removal or alteration of any "copyright management information." (17 USC §1202) It also prohibits the unauthorized distribution, importation for distribution or public performance of works from which such copyright management

information has been illegally removed. In addition, knowingly providing false copyright management information or distributing or importing for distribution false copyright information "with the intent to induce, enable, facilitate or conceal infringement" is also prohibited. (*Id.*)

By definition, protected copyright management information includes the following categories:

- The title or other identifying information, including the information contained on a copyright notice;
- The name or other identifying information about the author;
- The name or other identifying information about the copyright owner of the work;
- With the exception of public performances of works by radio and television broadcast stations, the name or other identifying information about the performer whose performance in fixed in the work;
- In the case of audio-visual works, with the exception of public performance of works by radio and television broadcast stations, the name and other identifying information about a writer, performer, or director credited in the work;
- The terms and conditions for use of the work (such as licensing contact information); and
- Any other information which the Register of Copyright may require.

Identifying information about end users is specifically excluded as a protected category of management information under the statute.

Similar to the anti-circumvention provisions, violations of information integrity may be challenged in both civil and criminal actions. Successful civil litigants are entitled to the full panoply of remedies, including statutory damages of not less than $2,500 nor more than $25,000 per violation. (17 USC § 1203) The markedly higher penalties imposed for violations of informational integrity, as opposed to technological protection measures, is due largely to the usefulness of copyrights management information as a tool for tracking pirated works, and the subsequent harm caused by its unauthorized removal or alteration.

Criminal violations require proof of willfulness and motivation for commercial advantage or private financial gain. (17 USC § 1204) First time offenders may be subjected to penalties of up to $500,000 in fines and/or

imprisonment for not more than 5 years. Recidivist penalties are significantly elevated. (*Id.*)

The only express statutory exceptions are for innocent violations, and for non-profit libraries, archives and educational institutions who had were "not aware and had no reason to believe that its acts constituted a violation." (17 USC §§ 1203(c)(5) and 1204(b)).

In *Kelly v. Arriba Soft Corp.,* 77 F. Supp.2d 1116 (SD Cal. 1996), *aff'd on other grounds,* 336 F.3d 811 (9th Cir. 2003), the court found that the failure to include digital rights management information in thumbnails versions of plaintiff's photographs, retrieved through the operation of defendant's visual search engine, was not a violation of the DMCA. The court held that the DMCA's prohibition against the knowing removal of such information did not apply because such the images at issue did not fall within the literal language of the statute. The DMCA prohibits removal of such information "conveyed in connection with copies or phonorecords of a work …" (17 USC §1202(c)). The court held that the thumbnails did not qualify as a "product" or "original work" under the statute. It further held that such removal was an "unintended side effect of the [defendant] crawler's operation," lacking any intent to violate plaintiff's rights. Finally, given the poor quality of the thumbnails the court held there was no reason to believe the removal of such information would lead to infringement of plaintiff's copyrights.

Temporary Copies

US copyright law has recognized that any temporary copy of a copyrighted work created in a computer environment qualifies as a reproduction for which permission is required from the copyright owner.

In its seminal decision, *MAI Systems Corp. v. Peak Computer, Inc.,* 991 F.2d 511 (9th Cir. 1993), the Ninth Circuit Court of Appeals held that a temporary copy created by booting a program into the Random Access memory of a computer qualified as a "copy" for which permission to reproduce the work was required by the copyright owner, even though the copy was not permanently "fixed." The court held that no permanent fixation was required since the definition of "copies" under the 1976 Act (as amended) is "material objects, other than phonorecords, in which a work is fixed by any method now known or later developed, and from which the work can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device," Since a person can load the software in question and then view the program, such reproduction was sufficiently permanent or stable to qualify as an unauthorized reproduction under the Act.

In *Religious Technology Center v. Netcom On-Line Communications Services, Inc.,* 907 F. Supp. 1361 (N.D. Cal. 1995), the court addressed what constitutes infringing reproductions in the context of the storage of digital information. Relying on the *MAI* case, the court held that "there is no question that after *MAI* that 'copies' were created, as [the user's] act of sending a message…. caused reproductions of the plaintiff's works." Ultimately, the court held that the display of recognizable copies through a computer was sufficiently permanent to constitute a copy under the Copyright Act.

Electronic Distribution Rights

The question of the right of publishers to translate freelance articles from print into a digital medium without additional compensation has been hotly contested.

In *Tasini v. The New York Times, 121 S.Ct. 1214 (2001),* the plaintiffs, free lance authors who had granted the defendants publication rights to their articles in printed periodicals challenged the subsequent sale by defendants of digital publication rights to these articles without additional compensation. The articles in question had appeared in collective periodical works by the New York Times. The digital versions at issue, however, appeared in digital databases which did not preserve the copyrightable aspects of the periodic publications in which the articles had originally appeared. The lower court held that the use by the New York Times of the articles was protected under Section 201(c) of the Copyright Act. This section grants copyright owners of collective works the "privilege of … any revision of [the] collective works," without further compensation to the author. (17 U.S.C. §201(c)) The Second Circuit Court of Appeals reversed and held that the digitized versions of plaintiff's articles did not qualify as a privileged "revision" under Section 201(c). Instead, given the nature of the works in the digital environment, including the fact that any such works did not duplicate the copyrightable elements of the collective work such as their selection and arrangement, the court held that reproduction in a digital database qualified as unauthorized duplication. The Supreme Court upheld the Second Circuit's decision that reproduction in a digital database did not qualify as an authorized "revision," but was, instead, an unauthorized reproduction.

Napster, Kazaa and Other "Facilitators"

Those parties which induce others to commit pirate activities may be liable for contributory copyright infringement. The most obvious "facilitators" who may be a target of a lawsuit are those who distribute software allowing peer to peer file transfers such as Kazaa and Napster. Under US law, a doctrine referred to as "the *Sony* doctrine" may present a serious limitation to the success of an action against any such third party facilitators.

Briefly in *Sony Corp. of America v. Universal City Studios, Inc.,* 464 U.S. 417, 429 (1984), the Supreme Court found that the manufacturers of video cassette recorders used to record broadcast television programs for time-shifting purposes were not liable contributory copyright infringement because such recorders were a staple article of commerce which had substantial non-infringing uses. Such non-infringing uses included the ability to engage in the reproduction of public domain materials, and the fair use reproduction of copyrighted works. Developed in the days of analog recording, the application of the *Sony* doctrine to those who facilitate unauthorized P2P file trading of copyrighted works is presently unclear.

The *Sony* defense has been held inapplicable in cases involving anti-circumvention violations. In *Universal City Studios, Inc. v. Reimerdes,* 111 F. Supp.2d 294 (SDNY 2000), *aff'd on other grounds sub nom. Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir. 2001), involving the DeCSS code for circumventing copy protection codes for DVD's, based on legislative history, court holds *Sony* doctrine does not apply to anti-circumvention provisions, although it remains a viable defense to contributory copyright infringement. Some courts have refused to use the *Sony* doctrine to excuse those who provide P2P software from contributory liability for the massive infringement that results from the easy and unsupervised availability of P2P file trading.

One of the largest technology based lawsuits in the United States in recent years was *A&M v. Napster,* 239 F.3d 1004 (9th Cir. 2001). The defendant, Napster, was engaged in the facilitation of peer to peer file trading of digital music files. In the late 1990's Napster ran a website that offered free downloadable copies of its software. This software allowed individuals to download musical compositions and sound recordings of copyrighted artists in MP3 format. It also allowed users to search and download MP3 files from any other user who is logged onto the Internet. In addition, Napster operated a search index which facilitated the searching and peer to peer transfer of digital music files between users. Napster argued that its actions did not qualify as copyright infringement since they merely facilitated the sharing of digital files. Alternatively the defendant argued that its actions were protected under the doctrine of fair use. The court rejected defendant's arguments and held that Napster's activities qualified as contributory copyright infringement. Moreover, since the end user's activities did not qualify as fair use, Napster's activities were not excused. The court ultimately held that Napster's actual knowledge of the infringing nature of its end users' acts vitiated any defense under *Sony*.

By contrast, in *Metro Goldwyn Mayer Studios, Inc. v. Grokster, Ltd*., 289 F. Supp.2d 1029 (C.D. Cal. 2003), the court found that the providers of P2P software could *not* be held liable for contributory infringement because they lacked "actual knowledge" of the infringing uses at the time that the end users downloaded the software in question. Similar to the *Napster* case, the *Grokster* decision involved the supplying the of free P2P file trading software. However,

unlike *Napster*, the facilitators in *Grokster* provided no search index and did not interpose themselves in the file transfer of end users beyond providing the software that allowed such file trading. Rejecting plaintiffs' claim for contributory copyright infringement, the court in *Grokster* emphasized that, unlike Napster, the facilitators in the *Grokster* case did not provide the "site and facilities" for its end users' infringing actions. The architectural differences between Grokster and Napster, in particular the fact that the software at issue "communicates across networks that are entirely outside the defendant's control" and the absence of a centralized file indexing system were considered critical distinctions.

The District Court's decision in *Grokster* was recently upheld on appeal in *Metro Goldwyn Mayer Studios Inc v. Grokster Ltd*., 2004 WL 1853717 (9th Cir. 2004). Relying on evidence that thousands of musical groups had authorized the free distribution of their music through the Internet and on the use of the software to trade public domain materials, the Ninth Circuit upheld the district court's finding that the P2P software in question was capable of substantial non-infringing uses. In light of these non-infringing uses, the court held that under the *Sony* doctrine the plaintiff would have to prove that the defendant had "reasonable knowledge" of specific acts of infringement. Constructive knowledge would be insufficient. The court rejected plaintiff's claim that the notices it sent established the requisite knowledge. The failure of Grokster to provide the "site and facilities" for infringement demonstrated that plaintiff's notices arrived "when defendants do nothing to facilitate, and cannot do anything to stop the alleged infringement." The court emphasized that P2P technology "is not simply a tool engineered to get around the holdings of [the *Napster* cases]. The technology has numerous other uses, significantly reducing the distribution costs of public domain and permissively shared art and speech, as well as reducing the centralized control of that distribution."

In another case involving P2P file sharing using instant messaging from a different circuit the court held that when a product or service has infringing as well as non-infringing uses "some estimate of the respective magnitudes of these uses is necessary for a finding of contributory infringement." In *In re Aimster Copyright Litigation,* 334 F.3d 643 (7th Cir. 2003), the defendant offered an encryption feature with its P2P software. This encryption prevented Aimster from knowing what files were being traded by its users. Such "willful blindness" was not sufficient to relieve the defendant of liability. While the court recognized that encryption fosters privacy, the court declined to allow such value to be controlling. In light of defendant's tutorial, which gave as its only example the sharing of copyrighted music, the court held the burden to "demonstrate that its service has substantial non-infringing uses" had shifted to Aimster. Furthermore, the court indicated Aimster must establish that the "primary use" of its system was to transfer non-copyrighted files. In the face of both non-infringing and infringing uses, Aimster was required to show that it would have been disproportionately costly for him to eliminate or at least reduce substantially the infringing uses." Describing Aimster's activities as an "ostrich-like refusal to

discover the extent to which its system is being used to infringe copyright," the court found such behavior "another piece of evidence that it was a contributory infringer."

As a result of the potential conflict between the *Grokster* and *Aimster*, the plaintiffs in *Grokster* have filed a petition for certiorari with the Supreme Court requesting that the court resolve the conflict regarding the secondary liability of P2P software providers under copyright law. The petition is currently pending.

In *UMG v. MP3.com*, 2000 US Dist LEXIS 13293 (S.D.N.Y. 2000), the defendant created an Internet service that allowed the public to download and copy MP3music files from their web site. The defendants alleged that they were merely engaged in the act of space shifting since they purportedly only allowed access to those digital files for which a user already owned a CD ROM copy of the song. The evidence, however, did not support this contention. Furthermore, the defendant had not obtained permission from the copyright owners of the songs in question to make the copies accessed by users. Having decided that the defendant had therefore infringed the plaintiff's rights, the court held that the defendants' actions were willful and wanton and held that statutory damages in the amount of $25,000 per CD infringed would apply.

In a case involving streaming video technology, the court in *RealNetworks v. Streambox*, 2000 US Dist LEXIS 1889 (D.Wash. 2000), held that plaintiff's streaming video VCR violated the DMCA but not its ripper, used to translate file formats. The plaintiff marketed various products that allowed end users to access audio and video content over the Internet through a process known as streaming. This process generally leaves no copy of the streamed work on the user's file. Plaintiff's products contained a copy protection measure which assured that only those files which the copyright owner has granted permission to be copied can be copied during the streaming process (referred to by the parties as a "secret handshake" and "copy switch" technology). Defendant's Streambox VCR did not incorporate this copy protection technology when streaming music files using plaintiff's RealMedia format. The court found that the Streambox VCR violated the DMCA's anti-circumvention prohibitions by failing to include these security measures. It rejected defendant's fair use defense, as well as defendant's contention that plaintiff's technology was not "effective." By contrast, however, it accepted defendant's fair use defense in connection with its "ripper" technology. This technology was used to translate files between various formats, including RealMedia, MP3 and . WAV. The court found that the RIPPER did not violate any anti-circumvention technology because the RealMedia *format* did not qualify per se as "technological protection measure" under the statute.

Enforcement Initiatives

Recent activities by the Recording Industry Association of America (RIAA) to combat illegal P2P file trading support the view that fool proof techniques are

not required to reduce pirate activities on the Internet. In a much publicized move last June, the RIAA, relying on Section 512(h) of the DMCA, 17 USC § 512(h), served subpoenas on diverse internet service providers seeking the identification of over 800 individuals the RIAA had identified as potentially possessing illegally copied music files on their computers. This activity was followed by the filing of 261 lawsuits nationwide in September, 2003, followed by additional cease and desist demands sent in November 2003. The subsequent spotlight on the issue of illegal file trading of copyrighted music, and the potential legal liability for such acts, appears to have had a marked effect on both the amount of piracy, and the number of individuals who are engaged in unauthorized file trading of music.[1] Recently the music industry reported its first positive growth in sales in four years. RIAA's enforcement activities remain on-going.

[1] *See, e.g.,* John Schwartz, "In Survey, Fewer are Sharing Files (or Admitting It)", New York Times (January 5, 2004)(reporting on apparent success of RIAA litigation strategy in reducing the numbers of end users who are file trading music illegally after the September lawsuits).