

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

---

**By Professor Doris Estelle Long\***

With an estimated 335 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. Because 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 on 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 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 the supporting 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

---

\* Professor of Law, The John Marshall Law School, Chicago, ILL, USA 60604. Copyright Doris Estelle Long 2001. This work may be freely reproduced for non-commercial, educational purposes so long as no changes are made in the text and the copyright notice is reproduced in full, along with the full author's credit contained herein.

(including digitally) to far flung customers. The rapid reproduction and distribution of IP-protected works, however, permitted by such technological advances 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.

## **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 an 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
- 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 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”).

One of the most significant defenses to a claim of copyright infringement is the defense of “fair use.” To consider 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 Millennium 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 than ever before and with a higher degree of 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 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) if it adopts and reasonably implements a

policy of terminating in appropriate circumstances the accounts of subscribers who are repeat infringers; (3) it accommodates and does not interfere with “standard technical measures” copyright owners use to identify or protect copyrighted works; and (4) if it meets other specified requirements regarding the particular activity in question (see below). The four activities for which safe harbor protection exists 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.

### *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.

### *Notice And Takedown Provisions*

---

As noted above, in order for an ISP to qualify for certain safe harbors, it must promptly remove infringing material as soon as it 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 of accuracy. (17 U.S.C. §512(c)(3))

These notice provisions allow the copyright owner a clear and concise way to communicate a cease and desist letter to the proper individual so that the infringing activity can be stopped as quickly as possible. This provision also helps puts all parties who may be part of the litigation on notice of allegedly infringing activity, thus eliminating any attempt to claim innocent infringement as a defense to monetary liability.

Where an ISP acts in good faith in response to a notice of infringement, it will not be liable so long as it takes reasonable notice to promptly notify the subscriber of its actions, provides the complaining party of any counter notification it receives from the complaining subscriber and replaces any removed material subject to a proper counter complaint within 10 to 14 days of receipt of the counter notice, unless the ISP receives notice from the original complaining party that it has filed a lawsuit regarding the material in question. (17 U.S.C. §512(g))

### **Anti-Circumvention Devices And Rights Management Information**

Under the Digital Millenium Copyright Act (DMCA) making or selling devices or services that are used to circumvent technological measures to prevent either unauthorized access or unauthorized copying of a copyrighted work are prohibited if such devices or services are primarily designed or produced to circumvent “technological protection measures.” The trafficking, manufacturing, importing or offering to the public such devices and services is also prohibited. (17. U.S.C. §1201)

These anti-circumvention prohibitions to not apply to the actions of law enforcement, intelligence, and other governmental activities. Non-profit libraries and educational institutions are also excepted. In addition, the prohibitions to not apply to the following activities:

- Reverse engineering
- Encryption research
- To protect minors from access to Internet material
- To protect personal privacy
- To protect the security of a computer, computer system or network (with the authorization of its owner or operator)

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. circumvention products and technologies. The fair use defense also does not apply to actions regarding the use of circumvention 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.

Section 1202 of the DCMA also prohibits the unauthorized removal or alteration of copyright management information. It also prohibits the knowing distribution of any work containing false copyright management information or containing copyright management information that has been altered or removed without permission. Where the defendant knows or has reasonable grounds to know that such distribution will induce, enable, facilitate or conceal an infringement of any right under the Copyright Act. "Copyright management information" includes not only information about the author/performer/copyright owner (including information contained in a copyright notice), but also information about the terms and conditions governing any use of the work in question. These prohibitions do not apply to the authorized actions of law enforcement, intelligence, and other governmental activities

The DMCA establishes both civil and criminal liability for violating the Anti-Circumvention and Rights Management integrity provisions of the Act, including statutory damages of up to \$2,500 per act of circumvention, device, product, component, offer or performance of service, and up to \$25,000 per rights integrity violation. (17 U.S.C. §1203)

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. Reimerdes*, 111 F. Supp. 2d 294 ( S.D.N.Y. 2000). In this case the court dealt with the liability of Shawn Reimerdes, better known as Emmanuel Goldstein, who runs 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 on the grounds that computer code did not qualify as speech. The decision is currently on appeal.

## **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 (9<sup>th</sup> 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 remains at issue.

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, MP3 and Other Digital Distribution Techniques**

One of the largest technology based lawsuits in the United States currently is *A&M v. Napster*, 239 F.3d 1004 (9<sup>th</sup> Cir. 2001). The defendant, Napster, is engaged in facilitation the peer to peer sharing of digital music files. The plaintiffs engage in the commercial recording, distribution and sale of copyrighted musical compositions and sound recordings. Napster runs a website that offers free downloadable copies of its software. This software allows individuals to download musical compositions and sound recordings of copyrighted artists in MP3 format. It also allows 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. The Defendants argued that their 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.

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 accesses by users. Having decided that the defendant had therefore infringed the plaintiff's rights, in this reported decision, the court determined what level of damages would be appropriate to compensate the plaintiffs. 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 *RIAA v. Diamond Multimedia Systems*, 180 F. 3d 1072 (9<sup>th</sup> Cir. 1999), the plaintiff sought to enjoin the defendant from manufacturing, selling and distributing the Rio. The Rio is a small device that allows a user to download MP3 audio files from a computer and listen to them, thereby increasing the portability of such files. Finding that the Rio is not capable of making copies from

digital “transmissions,” but instead, can only make copies from a computer hard drive, the court held that the Rio is not a digital audio recording device within the meaning of the Act. Consequently, defendant did not have to comply with statutory requirements that a “digital audio recording device” conform to the Serial Copy Management System (SCMS).

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 such 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.