A Brief Primer on U. S. Intellectual Property Protection in the Global Arena

By Professor Doris Estelle Long[*] and Nicole Milos[**]

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 in a global, digital environment. 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 are the Digital Millenium Copyright Act, the Federal Anti-dilution Act, and the Anti-Cybersquatting Consumer Protection Act.

Because a complete explanation of the protection of intellectual property in a global digital environment would fill hundreds of pages, this primer should not be considered a complete exposition of the intricacies of protection intellectual property on the Internet and in other digital environments. Instead, it should be considered as merely a snapshot view of present US protection trends in the area. This primer is intended some of the most important developments in the law. It 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

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

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 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.

In the United States the major areas of intellectual property law that have been used to deal with the problems and challenges posed by Internet and technology development in general are copyright, trademark and patent laws. Generally copyright protection has focused on the problems of protecting the content on the Internet. Trademark law has been used to deal with the problems of domain names; while patent laws have dealt with the questions of software and business method protection on the Internet.

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
- 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 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 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 to 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 (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 remains at issue.

In *Tasini v. The New York Times,* 206 F3d 161 (2d Cir. 1999), 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 case is currently on appeal before the US Supreme Court.

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 (9th 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 (9th 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.

US Trademark Law and the Internet

A General Introduction

Under US law a trademark includes "any word, name, symbol or device, or any combination thereof" which is used "to identify and distinguish" goods and "to indicate the source of the goods, even if that source is unknown." (15 U.S.C. §1127). The United States also protects service marks, collective marks and certification marks. Mark[1] protection in the United States has been extended to a

[1] For purposes of convenience only, the authors will use the term "mark" to refer to a source designator that can be protected under Federal Trademark Law. The term should be considered to include all types of protectable marks under US law, unless specifically noted to the contrary.

broad variety of source designators, including sounds, color, packaging and product configurations. Federal registration of a source designator is not required. Although registration provides many benefits, including nationwide constructive use and prima facie evidence of ownership and distinction, use in interstate commerce (without registration) is sufficient.

In order to qualify as a protectable mark, the commercial symbol must be either inherently distinctive, or have acquired distinctiveness, generally demonstrated through evidence of secondary meaning. In addition the mark must be used in connection with the relevant goods or services in interstate commerce. Thus, for example, a domain name, per se, does not necessarily qualify as a protectable *mark,* since it is nothing more than an Internet address for a web page. When the domain name is used in connection with goods or services, however, such as for a web page that also permits customers to order goods from the site, it may qualify as a source designator subject to protection under US trademark law.

The heart of US Trademark law is the protection of the public from likely confusion that may result from the unauthorized use of "confusingly similar" marks by unauthorized third parties. In order to recover for mark infringement, the owner must prove that the unauthorized use "is likely to cause confusion or mistake or to deceive as to the source of origin or such goods and services." In order to determine likelihood of confusion, courts consider a variety of features, including:

- The similarity of sound, appearance and meanings between the marks:
- The similarity of the channels of trade and distribution between the marks;
- The similarity of the goods and services;
- The strength of the marks, including the prevalence of use of similar marks by other third parties;
- The quality of the goods or services;
- The mark's reputation may be tarnished by such use;
- The good faith adoption of the second comer;
- The sophistication of the customers; and
- The existence of actual confusion arising from the unauthorized use of the mark.

US Trademark law provides for a complete panoply of remedies for mark infringement, including injunctive relief, seizure and destruction of the infringing copies as well as all labels, signs, prints, packages, wrappers, receptacles and advertisements in the possession of the defendant bearing the mark, and the means for making them, actual damages (including lost profits), statutory damages for counterfeit marks, up to $1,000,000 per counterfeit mark per type of goods sold for willful infringement, costs and reasonable attorney's fees.

Dilution

The Federal Trademark Dilution Act (FTDA), which is codified as part of the Lanham (Federal Trademark) Act, protects famous marks against unauthorized uses in commerce of similar marks that "cause dilution of the distinctive quality of the mark." (15 U.S.C. §1125(c)) Dilution is defined by statute as "the lessening of the capacity of a famous mark to identify or distinguish goods or services." Courts are currently split over whether actual dilution or simply a likelihood of dilution must exist for relief under the statute. Unlike trademark infringement, relief under the FTDA does not require any finding of likelihood of confusion between the two marks at issue.

In order to determine whether a mark qualifies as "famous," the FTDA establishes eight non-exclusive factors which courts should consider, including:

- The degree of inherent or acquired distinctiveness of the mark;
- The duration and extent of use of the mark in connection with the goods or services with the mark is used;
- The duration and extent of advertising and publicity of the mark:
- The geographical extent of the trading area in which the mark is used;
- The channels of trade for the goods or services with which the mark is used;
- The degree of recognition of the mark in the trading areas and channels of trade used by the marks' owner and the person against whom relief is sought;
- The nature and extent of use of the same or similar marks by third parties;
- Whether the mark is federally registered on the Principle Register.

(15 U.S.C. §1125(c)(1)) The statute excepts fair and non-commercial uses of a mark, as well as all forms of news reporting and news commentary, from its prohibitions.

Relief for trademark dilution is limited to injunctive relief, except in instances of a "willful intent to trade on the owner's reputation or to cause dilution" in which case actual damages, attorney's fees, costs and destruction of

the infringing articles and any means for making the same may be seized and destroyed.

The Federal Trademark Dilution Act has been used frequently in order to obtain relief against unauthorized uses of trademarks and domain names on the Internet. Thus, for example, in an early decision, *Panavision v. Toeppen* 141 F. 3d 1316 I(9th Cir. 1998), the court used the Federal Trademark Dilution Act to prohibit the unauthorized reservation of a domain name containing plaintiff's famous mark. The defendant had registered trademarks on the Internet as Domain Names and then attempted to extort money from companies like the plaintiff who owned the mark. The court held that under the "effects doctrine," the court had personal jurisdiction in California over defendant's activities. The court recognized the defendant's scheme to register already established trademark names in an attempt to solicit money from the rightful trademark owner qualified as an unauthorized use in commerce for which relief was available under US law.

Anti-Cybersquatting Consumer Protection Act (ACPA)

Although mark owners had been relatively successful in using the Federal Trademark Dilution Act to combat the activities of cyber-piracy, the unique nature of domain names continued to pose problems for mark owners. Consequently, in 1999 the Anti-Cybersquatting Consumer Protection Act was enacted to allow rightful mark owners to bring a suit against the bad faith registration, trafficking or use of infringing domain names. Under the ACPA, trademark owners may now bring an action against a person who, with a bad faith intent to profit, registers , uses or traffics in a domain name that (1). is identical or confusingly similar to a mark that was distinctive when the domain name was registered; or (2). is identical or confusingly similar to or dilutive of a mark that was famous when the domain name was registered. The statute specifies a variety of non-exclusive factors that should be considered in determining whether the plaintiff acted in bad faith. These factors include:

- IP rights of the person in the domain name;
- Whether the domain name is the name of a person;
- Proof of a prior bona fide use;
- Noncommercial and fair use of a mark in the site by the person;
- The person's intent to divert consumers from the mark's original owner;
- The person's offer to sell the domain name to the mark owner;
- The persons provision of material or misleading contact information;
- The person's registration or acquisition of a multitude of similar or identical domain names;
- The extent of the mark's fame and distinctiveness.

No bad faith intent can be found where the court determines that the person "believed and had reasonable grounds to believe that the use of the domain name was a fair use or otherwise legal." (15 U.S.C. §1125(d)(1)(B)(ii))

To assure that mark owners will be able to obtain jurisdiction over cybersquatters the ACPA provides for in rem jurisdiction in the judicial district in which the domain name authority that registered or assigned the Domain Name is located. . Remedies available under the ACPA include actual damages, statutory damages up to $100,000 per domain name, injunctive relief and forfeiture, cancellation or transfer of the domain name to the mark owner. Remedies in an *in rem* proceeding are limited to the forfeiture, cancellation or transfer of the domain name to the mark owner.

Domain Names, Metatags and Search Engines

While the ACPA has provided new legal precedents to apply in resolving domain name disputes, it should be noted that the statute is relatively limited in scope. Its prohibitions only apply in situations of cybersquatting. Other domain name conflicts are generally handled under traditional trademark infringement or dilution analysis.

The protection of trademarks from their unauthorized use as metatags and keywords for Internet search engines has also generated a great deal of legal debate. The use of similar domain names for parody and slam sites has generated a great deal of debate.

Thus, for example, In *Bally Total Fitness Holding Corp. v. Faber,* 29 F. Supp. 2d 1161 (C.D.Cal. 1998), the court allowed the use of the mark "ballysucks" in connection with a website dedicated to consumer complaints run by a disgruntled former customer. In *Bally,* the defendant maintained a website critical of plaintiff's health club business. The site presents the viewer with the Bally trademark with the word "Sucks" printed across it. Although the court recognized that Bally's mark was quite valuable, it held that the use of the mark by Faber produced no likelihood of confusion. It also refused relief under the FTDA, finding that defendant's use of the Bally mark did not qualify as a commercial use, therefore, the court granted Faber's motion for summary judgment on trademark infringement. In addition the court held that Faber's use of the trademark is not a commercial use because it was not used to advertise or promote his own services. The court also found no tarnishment defendant's site contained consumer commentary, which is protected under the First Amendment.

Similarly, in *Bihari v. Gross* 119 F. Supp. 2d 309 (S.D.N.Y. 2000) the defendant, a dissatisfied former client of plaintiff's interior design services established websites critical of the plaintiff, using the names "Bihari" and "Bihari interiors" in the domain names and metatags for their websites. Plaintiff sought

an injunction to stop the defendant. Analyzing plaintiff's claims under the ACPA, the court held that the prohibitions of the ACPA do not apply to metatags. The request for a preliminary injunction was denied. The court held that the plaintiff failed to demonstrate any likelihood of success on the merits of its Lanham Act claim because the defendant's use of the plaintiff's mark in the metatags was not likely to cause confusion. In addition, the court found that defendant's use was protected as a fair (non-source designating) use.

The question of potential trademark confusion arising from the use of metatags composed of another's mark has also been the subject of numerous court decisions and disputes.

In *Playboy Enterprises, Inc. v. Netscape Communications Corp.,,* 55 F. Supp. 2d 1070 (C.D.Cal. 1999), the Central District Court of California found that use of plaintiff's famous mark as a metatag for defendant's site qualified as trademark infringement. Metatags are keywords or phrases that can be inserted in the HTML code of a website. They are invisible to the human eye but are used by search engines in selecting the websites to be displayed in response to a user's search request. In this case, the defendants had provided metatags "playmate" or "playboy" to locate various adult entertainment sites they operated on the web. Playboy argued that allowing for the registration and recognition of keywords like "playmate" and "playboy" violated their trademark rights under the Lanham Act. The court held that although the defendants were using the trademarks in questions as metatags, such use qualified as a fair use since the use in question did not lead to any likelihood of confusion, or tarnishment or blurring of plaintiff's famous mark. .

By contrast, however, in *Brookfield Communications, Inc. v. West Coast Entertainment Corp.,* 174 F. 3d 1036 (9th Cir. 1999), the court found "initial interest confusion" in the unauthorized use of the "moviebuff" metatag and domain name for defendant's website with a searchable entertainment database. The plaintiff Brookfield gathers and sells entertainment industry information. It uses the trademark "moviebuff" in connection with its software and on-line database concerning information in the field of motion picture and television industries. The defendant operated a movie rental store and had previously registered "moviebuff' as a domain name for its movie information website. Rejecting the defendant's claim of prior rights in the term based on its prior registration of the term "moviebuff," for its software and on-line information services, the court instead focused on whether the use of the domain name and metatag in question would lead to initial interest confusion. Such confusion arises when the customers realize that the Internet site they have accessed is not the one they were looking for. Applying initial interest confusion, the court found that defendant's use of the domain name moviebuff.com and the moviebuff metatag lead to such confusion.

The doctrine of initial interest confusion and, more precisely, its application to various types of metatags, however, remains hotly debated.

US Patent Law and the Internet

A General Introduction

US Patent law, patent protection is extended generally to "any new and useful process, machine, manufacture or composition of matter, or any new and useful improvement thereof." (35. U.S. C. §101) To qualify for protection an invention must be novel, non-obvious and useful. (35 U.S.C. §§ 102, 103) It must be also granted patent protection through an application process before the US Patent and Trademark Office. During the examination process the invention will be reviewed to determine whether it meets the tri-partite test under US law for patentability. In addition, the applicant must disclose the best method for practicing the claimed invention as of the date of application. Under current law, applications are published 18 months after application.

A patent owner is given the right to exclude anyone from making, using, selling, offering to sell or importing his patented invention. Protection is also extended to process patents, plant patents and design patents. A panoply of remedies is available, including injunctive relief, actual damages, including, for example, a reasonable royalty for the use made of the invention, costs and attorney's fees.

The most significant use of patent protection in connection with technological innovation and the Internet currently appears to be the extension of protection to so-called business methods. It should be noted that no special test has been developed in connection with business methods patents on the Internet. Instead, the method must meet the standard tri-partite requirements of novelty, non-obviousness and usefulness. Nevertheless, because of the increasing number of business method patents being granted in connection with new business models on the Internet, Congress has recently begun to examine the scope of such protection.

Business Methods Patent on the Internet

In the seminal decision, *State Street Bank v. Signature Financial Group,* 149 F. 3d 1368 (Fed. Cir. 1998), the Federal Circuit Court of Appeals addressed the application of patent protection to a business method for hub and spoke asset pooling and investment. The court put to rest the bias that had previously been held against business methods patents, reaffirming that the "business" related subject matter of the invention should not have any effect on its patentability. Instead, the patent should be measured by the statutory elements of Section 101 of the US Patent Act.

The *State Street* decision impacted US patent law on many levels. Most importantly, the decision confirmed the categorical requirements for patentability set forth in the US Patent Act as the sole factor in deciding patentability. Until this decision, much of the material now being sought to be protected under a business method patent was kept private as a trade secret within a company. With the promotion of patent protection for these and similar issues, information can be put into the public domain and other businesses can reap the rewards of the knowledge gained by patents like these.

One of the most recent examinations regarding the scope of protection to be afforded a business method patent is *Amazon.com, Inc. v. BarnesandNoble.com, Inc.,* 239 F. 3d 1343 (Fed. Cir. 2001). Amazon sued Barnes and Noble for infringing its rights in a business method patent covering Amazon's one-click or express lane shopping method used on its retail Internet website. Amazon was granted a preliminary injunction against Barnes and Noble, prohibiting Barnes and Noble from continuing to conduct sales using their allegedly infringing business method of one-click ordering. In this recent decision, the court reversed the earlier grant of preliminary relief. The court found that defendants had provided substantial evidence regarding the potential invalidity of the patent in suit based on diverse prior art references. Consequently, the preliminary injunction was lifted pending further litigation.

Pending Business Methods Patent Legislation

Because of the concern that has been raised over the ability to determine the patentability of business methods, legislation has been proposed to address some of the criticisms raised. Entitled the "Business Method Patent Improvement Act of 2000," this new act attempts to address in particular the contention that business method patents do little more than grant monopoly protection to commonly used market tools. The bill defines those operations that could be included as a business method and alters the obviousness standard for such methods. This new standard would place a presumption of obviousness on the proposed invention when a prior art reference, "differs from what is claimed only in that the claim requires a computer technology to implement the practice of the business method invention." Applications for a business method patent would be published 18 months after the filing date. In addition, the bill reduces the burden of proof imposed upon the patent challenger, by raising the invalidity threshold to a preponderance of the evidence. It is too soon to determine whether this proposal will be adopted.

Frequently asked questions

Q. Under US Law, how do I know if my actions of uploading or downloading a document, song or movie constitute a copyright violation?

A. With certain limited exceptions arising under the fair use doctrine it is generally a violation to upload or download copyrighted materials without the permission of the copyright owner. Since authors are not required to place a copyright notice on their materials for copyright protection to attach, you should not assume that the absence of a notice means the work is in the public domain and therefore available to be freely copied. You should also not assume that because is work is available on the Internet, you are entitled to freely copy and distribute the work. Many pirated works are on the Internet, Thus, the mere fact that a work appears on the Internet does not mean you can copy or distribute it without the permission of the copyright owner.

Q. How can I, as an Internet Service Provider located in the United States, protect myself from liability if my end users violate applicable copyright laws?

A. Title II of the Digital Millenium Copyright Act (DMCA) insulates ISPs from money damages for the infringing activities of their users if they are involved in one of four “safe harbor” activities. These activities are: serving as a non-interactive conduit for Internet communications, caching, storing end user’s web materials and providing hyperlinks and other research tools. In order to qualify for these “safe harbors,” an ISP hosting an allegedly infringing page or site must have little or no involvement with the content of the allegedly infringing page or site. The ISP must also make it easy for copyright owners to contact it to provide information about alleged infringements and must act promptly to remove the infringing materials from the server on receipt of a proper notice. The ISP must have the technical expertise and authority necessary to locate allegedly infringing pages or sites, identify their owners, disable access to them and re-enable access to such sites if they receive an appropriate counter-notice.

Q. How do I secure a domain name in the US?

A. One of the most important domain name registers in the United States is Network Solutions, Inc. (NSI). NSI administers the .com domain (among others). You can usually apply to your Internet Service Provider (ISP) for a domain name to be registered with NSI. Some important points to remember when filling out the application are:

- Make sure that the name you are requesting follows the naming structure ("www" should not be entered as part of the domain name).
- Indicate "New" as the registration type in line one of the application.

- .Fill in all lines and do not abbreviate or use the term "same."
- Put "Request for new domain: my-domain.city-name.state.us" in the subject field.
- Submit the application via email to usdomreg@nic.us.

Q. Can I secure a domain name if I do not own the trademark that I want to use as my domain name?

A. Securing the domain name of an already established trademark can lead to trouble. The Anti Cybersquatting Consumer Protection Act (ACPA) allows a person to file a civil action against a person who, “registers, traffics in, or uses a domain name that - ":

I. in the case of a mark that is distinctive at the time of registration of the domain name, is identical or confusingly similar to that mark;

II. in the case of a famous mark that is famous at the time of registratio of the domain name, is identical or confusingly similar to or dilutive of that mark; or

III. is a trademark, word, or name protected

with an intent to profit from the mark (bad faith). Registering the domain name alone is sufficient to violate the Act. The web page does not have to be launched. In addition to being ordered to cancel or transfer the domain, an unsucessful defendant may also be ordered to pay money damages, attorney’s fees and costs.

Q. Are all Internet business methods patentable?

A. According to the *State Street* decision, the patentability of business methods is no easier that patenting any other type of invention. The proposed invention must still meet the tests of novelty, usefulness and non-obviousness as defined by the Patent Act. Until this decision, much of the material now allowable as a business method patent was kept private as a trade secret within a company. This decision promoted patent protection for these methods and, therefore, helped place information about these methods in the public domain so that other businesses can reap the rewards of the knowledge gained by these patents.