# HANDLING INTELLECTUAL PROPERTY ISSUES IN BUSINESS TRANSACTIONS:

# E-BUSINESS SOLUTIONS TO P2P PIRACY: A PRACTICAL GUIDE

Doris Estelle Long

# Biographical Information

Program Title: Handling Intellectual Property Issues in Business Transactions

Name: Doris Estelle Long

Position or Title: Professor of Law

Firm or Place of Business: The John Marshall Law School

Address: 315 South Plymouth Court, Chicago, IL

Phone: 312 360 2651

Fax: 312 427 9974

E-Mail: 7long@jmls.edu

Primary Areas of Practice: Intellectual Property, Unfair Competition, International Intellectual Property, Internet

Law School: Cornell Law School

Work History:

The John Marshall Law School

The Office of Legislative and International Affairs, US Patent and Trademark Office

Arent, Fox, Kintner, Plotkin & Kahn

Howrey & Simon

Membership in Associations, Committees, etc.: Professor Long is a frequent lecturer in the areas of intellectual property law, e-commerce. culture and technology, and has presented papers at conferences in such diverse places as

Havana, Cuba; Beijing, PRC; Moscow, Russia; Santo Domingo, Dominican Republic; Lima, Peru; Kathmandu, Nepal; Rio de Janeiro, Brazil; Dakar, Senegal; Chiang Rai, Thailand; Taipei, Taiwan; Warsaw, Poland; Kiev, Ukraine; Chisinau, Moldova; Guinea, West Africa and New Delhi, India. She is the author of numerous books and articles in the area of intellectual property law, including a treatise entitled *Unfair Competition and the Lanham Act.* Among her most recent articles are *Globalization: A Future Trend or a Satisfying Mirage?, The Protection of Information Technology in a Culturally Diverse Marketplace* and *The Impact of Foreign Investment on Indigenous Culture: An Intellectual Property Perspective.* She is also the co-author of the *Coursebook in International Intellectual Property* published by West. Professor Long is also a co-editor and contributing author of two anthologies: *International Intellectual Property Law Anthology*, and *International Intellectual Property Law*, and a textbook *Contracts Law and Practice: Cases and Materials*.

## Introduction

This Article explores the practical business, technological and legal solutions that can be used to address the growing problem of piracy, and particularly peer to peer ("P2P") piracy, on the Internet. It examines the trends which drive intellectual property enforcement on the Internet and discusses the growing reliance on technological protection measures, including the anti-circumvention and information integrity provisions of the Digital Millennium Copyright Act ("DMCA"). This Article briefly discusses recent legal developments in the US regarding the pirating of copyrighted works on the Internet. It examines e-business models for combating P2P piracy and calls attention to the growing successful reliance on fair use and free speech defenses in Internet piracy cases. This Article concludes by providing practical suggestions for developing an anti-piracy program to combat illegal P2P file trading of copyrighted works, and for dealing with piracy issues within the context of diverse business transactions.

"Ripping" movies, "burning CD's," "warez" sites, "Napsterites," peer to peer file "sharing," -- Internet piracy has become so prolific that it has developed its own shorthand for referring to such illegal activities as the unauthorized global reproduction and distribution of music, films, software and other copyrighted works on the so-called "Digital Information Highway." Initially, Internet pirates were concerned primarily with the unauthorized distribution of third party computer software. As compression technology improved, however, recorded music became an increasing target for pirate activity. Now, even full length movies are routinely copied and "traded" by cyberpirates. Size is no longer a deterrent to pirate activities. In short, no category of copyright protected work is safe.

Moreover, Internet piracy is not limited to teenagers, college students or "techno-geeks." To the contrary, Internet piracy apparently knows no boundaries in class, education or even age (except, perhaps, the pre-literate). Pre-teens to grey haired grandparents engage in the downloading of unauthorized copyrighted works. Their choices of subject matter may vary, with the younger favoring movies and songs, while the older favor recipes, sewing patterns and photographs. Even their chosen method of distribution may vary, with the elderly largely relying on email, while the younger run their own websites. Yet they apparently are all engaged in exponentially increasing numbers in the unauthorized reproduction and distribution of copyrighted works. While piracy of music, films and software receives the lion's share of public attention, the reality is that even copyrighted quilting and sewing patterns are being pirated by grey-haired grannies.

It is axiomatic that any business transaction that involves the development, transfer or commercialization of copyrighted works nowadays must address measures and responsibilities for combating the nearly guaranteed electronic piracy of

those works. The need to establish business methods and practices to combat piracy is particularly acute in those business transactions that involve copyrighted works which will be marketed to the general public, whether as a stand alone product (such as a music CD) or in combination with other products (such as an instruction manual). Given the wide-spread incidence of Internet piracy, parties to any business transaction involving copyrighted works would be well-advised to consider the issue.

*The Scope of the Problem*

*What is Internet Piracy?*

"Piracy" is generally considered to be the unauthorized reproduction of virtually identical copies of copyrighted works. "Counterfeiting" by contrast concerns the unauthorized use of virtually identical ("spurious") trademarks on the same types of goods as those for which the mark is used by the legitimate mark owner. "Internet", "digital," or "cyber-" piracy generally refers to the unauthorized distribution of virtually identical copies of copyrighted works by use of the Internet or other digital media.

There are numerous ways in which Internet piracy occurs. The most prevalent methods include:

1. Offering free or minimal cost pirated copies on a website for download. One of the most prevalent examples are the "warez" sites that offer minimal fee downloads of copyrighted software. "Charitable" pirates, such as university students often run "free" websites with copies of the latest software, films, or music available for free.[1]

[1] I refer to them as charitable pirates because unlike warez site operators, these pirates seek no financial gain for their activities. To the contrary,

2. Offering digital storage web services that allow end users to "space shift" their copyrighted works from disc media to computer media. The most notorious example of this type of service is the My MP3.com website which allowed end users to upload copies of CD music onto their server for easy access from anywhere in the world where Internet service was available. (*See UMC Recordings, Inc. v. MP3.com, Inc.*, 92 F. Supp.2d 349 (S.D.N.Y. 2000))

3. Peer to Peer (P2P) File Sharing. This type of file sharing has become the most prevalent method for end user piracy of consumer goods such as software, films and music. Peer to Peer sites are generally modeled on two methods of distribution:

   The Napster Method

   This type of website offers free software necessary to affect the peer to peer transfer. It also assists in such file transfers by operating an indexing system that makes the desired files easier to locate. Since the decision in the *Napster* case holding Napster contributorily liable for copyright infringement for running such a software and indexing site, however, the popularity of these types of sites has rapidly diminished. (See *A&M Records Inc. v. Napster, Inc.*, 284 F.2d 1091(9th Cir. 2002)). The Napster Method has been replaced by the Kazaa Method.

---

they give the works away for free (hence the "charitable" nature of their activities). Of course the works they are so willing to give away do not belong to them. Hence the term "pirate."

The Kazaa Method

This type of website offers free software necessary to effect peer to peer file transfers, but does not otherwise become involved in facilitating such transfers. Recently, the US District Court in *Metro-Goldwyn Mayer Studios Inc. v. Grokster,* 289 F. Supp.2d 1029 (C.D. Cal 2003), held that Kazaa's activities in simply providing P2P software, without more, did not qualify as contributory copyright infringement. The case remains on appeal at the time this Article was written. The present refusal to extend liability to the providers of P2P software for the infringing acts undertaken using the software apparently has lead to a greater willingness by some copyright holders to sue end users directly for copyright infringement. This development in turn has led to a newer type of peer to peer file trading network, one that offers not merely the P2P software, but anonymity for file traders as well.[2]

4, Emails, bulletin boards and chat rooms. The distribution of pirated works is often furthered through subsequent distribution by end users to others through electronic email, bulletin board and chat room services operated via the Internet.

Although the focus of this Article is Internet piracy, copyright infringement via the Internet and other forms of digital technology is *not* limited to the unauthorized reproduction and distribution of literal copies of protected

[2] *See, e.g.,* Saul Hansell, "Crackdown on Copyright Abuse May Send Music Traders Into Software Underground," New York Times (September 15, 2003)(discussing growth of Blubster and other sites which offer P2P software that provides mechanisms for anonymous trading of files, including encryption).

works. Among the other forms of copyright infringement using digital technologies which are currently most prevalent are:

1. The unauthorized digital manipulation of copyrighted works to create derivative or enhanced versions of the original. Such derivative versions may then be offered in competition with the original.

2. The unauthorized digital distribution of hard copy works, such as the digitally distributed copies of the New York Times articles that were the subject of the *Tasini* lawsuit. (*See New York Times Company, Inc. v. Tasini* 533 US 483 (2001) )

3. The unauthorized creation and distribution of derivative versions of copyrighted works. Such derivative versions may include the creation and use of digital sampling, and virtual and hard goods collages. It also includes the creation and posting of excerpted versions of songs, films and television shows, and scripts on fan sites, as well as parodies, take offs, knock offs, and other "fan" or critical postings.

4. The unauthorized creation and distribution of indexing materials, metatags and other source location materials to assist in the retrieval of information from the Internet, including by use of search engines. As a general rule, such information retrieval activities have been upheld. (*See Kelly v. Arriba Software Corp.*, 280 F.3d 93 (9th Cir. 2003)(upholding as a fair use the unauthorized reproduction of photographs by a visual search engine and the provision of thumbnail versions of such photographs to end users ).)

While such copyright infringing activities are not the focus of this Article, any business transaction which deals with copyright protected materials should also consider the potential for these types of unauthorized uses for the assets involved, and should use techniques similar to those described here for combating such infringements.

*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. Industry surveys demonstrate that shipments of recorded music in the United States have dropped 26% since 1999.[3] Last year, about 1.8 billion blank CD's were sold, compared to 800 million recorded CD's.[4] Not even independent companies are immune to the adverse economic effects of illegal file sharing.[5] Whatever the exact figures, it is undeniable that Internet piracy presents a serious challenge to traditional methods for protecting copyrighted works in a digital environment. As technology advances, so 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 illegally traded over the Internet through P2P file sharing.

---

[3] *See, e.g.*, Not-so-Jolly Rogers, The Economist (September 10, 2003).

[4] *See, e.g.*, Mark Landler, "US is Only the Tip of Pirated Music Iceberg," New York Times (September 25, 2003).

[5] *See, e.g.*, Chris Nelson, "Upstart Labels See File Sharing as an Ally, Not Foe," New York Times (September 22, 2003)(reporting that in 2002 album sales dropped 17.3% with file sharing and illegal CD burning contributing to the drop).

Countless factors have contributed to this increasing problem. One of the most significant contributing factors to the growth in 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 P2P file sharing, and providing potentially hundreds of copies of a favorite digital song to strangers, does not adversely affect the ability of the "helpful trader" to continue to enjoy that song. Unlike the old days, an illegal file trader 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 trade it too with no inconvenience whatsoever.

Further fueling Internet piracy is an increasing "disconnect" in end users' and website owners' minds between physical theft and electronic theft. People who would never engage in shoplifting have no compunction in making and distributing illegal downloads of copyrighted songs.[6] There is an ethical chasm between the two activities which cannot be bridged by laws alone.

Digital piracy is also relatively inexpensive. With the growth of Internet cafes globally, would-be pirates no longer

---

[6] *See, e.g,* Katie Hafner, "Is it Wrong to Share Your Music?," New York Times (September 18, 2003)(reporting on diverse views among junior high students regarding their right or intention to continue downloading illegal music); Laura M. Holson, "Studios Moving to Block Piracy of Films Online," New York Times (September 24, 2003)(reporting on focus group meeting with college and high school students where participants indicated an intent to continue illegally downloading films regardless of legal prohibitions).

need to invest in expensive computers or duplicating machines to fuel pirate enterprises. Sufficient money to pay for Internet access fees, and one disc of recordable memory, is sufficient. Moreover, 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. However, countless others, such as the now-largely dismantled Napster (at least in its old guise as a P2P free trading network[7]) and Kazaa 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.

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 copyrighted songs from music CD's, or copyrighted films from DVD's. To the contrary, given the wide-spread existence of pirated films and music on the Internet, there may not be currently an even mildly effective copy protection technique.

Given past history, I seriously doubt that any "foolproof" technology will ever be created. No matter how sophisticated the technique, somewhere in the world there is some computer hacker (usually under the age of 20) who will be able to circumvent whatever technique we can create. But "foolproof" methods are *not* required. *Effective* methods, methods which are capable of discouraging all but the hard-

---

[7] Napster re-launched itself at the end of 2003 as a legitimate distributor of digital music. *See, e.g,* Penn State, "Napster Ink Pact," Wired News (November 6, 2003) at http://www.wired.com/news/digiwood/html) (reporting on agreement between newly launched Napster and Penn State to provide legal music downloading services to university students).

core pirate, are what is needed. These methods may be attainable.

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.[8] This activity was followed by the filing of 261 lawsuits nationwide in September, 2003,[9] followed by additional cease and desist demands sent to 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.[10]

The absence of a current technological solution to piracy is coupled with a growing perception that "fair use" is a right and not merely an occasional exception to a copyright owner's rights. Such fair use right is rapidly being

---

[8] *See, e.g.,* "Music Industry wins approval of 871 subpoenas," AP Newswire (July 21, 2003)(reproduced at http://edition.cnn.com/2003/TECH/Internet/07/21/downloading .music.ap/index.html). For details regarding the current legal status of subpoenas under the DMCA, *see* discussion below.

[9] *See, e.g., "*Hundreds of Music Swappers Sued," Associated Press Newswire (September 8, 2003)(reprinted at www.msnbc.com/main.story) (reporting on institution by RIAA of 261 lawsuits against end users based on illegal P2P file trading).

[10] *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).

transformed into a right to make a copy of a work from the Internet "just because you want to." Thus, even when copyright owners attempt to protect their works through technological measures (such as in the case of the anti-circumvention measures contained in the Digital Millennium Copyright Act discussed in greater detail below), they face an increasingly organized public protest against such enforcement. Such organized opposition has led to the introduction of bills in the US Congress that seek, among other developments, to grant end users a virtual compulsory license to download songs from the Internet. Such public protests can also be directly linked to the dismissal of criminal charges against Dimitry Skylarov in 2002 for creating a software program designed to circumvent copy protection codes for e-books, and to the ultimate failure of the prosecution against Skylarov's employer.

Finally, until July 2003, engaging in digital piracy was perceived to be a generally risk free activity. End users were rarely prosecuted under the theory that they are "potential customers." Even those who operate commercial pirate sites rarely faced litigation to end their activities. Until recently, the only notable exceptions to this non-litigation strategy appeared to be websites such as Napster and Kazaa that offered freely downloadable P2P software. The District Court's decision in *Metro-Goldwyn Mayer Studios Inc. v. Grokster,* 289 F. Supp.2d 1029 (C.D. Cal 2003), and the Dutch Court's recent decision in a related case in the Netherlands[11], both of which refused to impose liability on Kazaa for the infringing acts of end users, may signal an end to the focus on P2P software distributors. Both cases are currently on appeal.

---

[11] *See, e.g,* "Dutch Court Says Kazaa Not Liable for Copyright Infringement," Associated Press Wire (December 20, 2003)(reprinted www.iht.com/articles/12266.htm) (reporting that the Dutch Court has found Kazaa not liable for contributory copyright infringement for the distribution and use of its P2P file trading software).

*Internet Piracy: Current Legal Developments*

Under US copyright laws, copyright owners have the exclusive right to do and to authorize the following;

1. To reproduce the copyrighted work;

2. To prepare derivative works based on the copyrighted work;

3. To distribute copies of the work to the public by sale or other transfer of ownership, or by rental, lease or lending;

4. To perform the copyrighted work publicly;

5. To display the copyrighted work publicly; and

6. In the case of sound recordings, to perform the copyrighted work publicly by means of a digital audio transmission. (17 USC § 106).

Infringement occurs whenever anyone infringes any one of these bundled rights. Literal copying is not required. In addition to direct infringement, courts recognize claims for vicarious and contributory infringement. Thus, the person who induces another to infringe someone's rights, or who assists in such infringement (such as by producing the illegal goods at the request of another) is equally liable. Persons are liable for contributory infringement if they have knowledge of the infringing activities and induce, cause, or materially contribute to such activities. Persons are liable for vicarious liability if they have the right and ability to supervise the parties engaged in the infringing activities and have a direct financial interest in the exploitation of the

copyrighted work. (*See generally A&M Records, Inc. v. Napster, Inc.*, 284 F.2d 1091 (9th Cir. 2002).)

Proving copyright infringement under US law essentially requires evidence of (1) ownership, (2) unauthorized copying and (3) substantial similarity of protectable expression in the works. If the copyright owner is a US author, he must register the work with the US Copyright Office before filing suit. A copyright registration certificate serves as prima facie evidence of copyright ownership and of the copyright protectable nature of the work.

Unauthorized copying, or other unauthorized uses of copyrighted works, is rarely demonstrated through direct evidence. However, in cases of Internet piracy, the substantial identity of the works, along with evidence of lack of authorization is sufficient.

The remedies available in civil cases for copyright infringement under US law include injunctions, damages, attorneys' fees and costs, and impoundment or destruction of infringing materials. In cases of Internet piracy injunctions against continued access to the website at issue have proven particularly effective. In lieu of actual damages, the copyright holder can elect to receive statutory damages) that are equal to a sum of not less than $750 or more than $30,000 per infringement. If the court finds the infringement willful (which usually occurs in cases of piracy), it can award up to $150,000 in statutory damages per infringement.

*1.* *No Electronic Theft 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.

2. *Potential Defendants*

Among the potential violators in the chain of production and distribution of a pirated work on the Internet are Internet Service Providers ("ISP's"), the operators of websites where illegal content is posted, end users, and "facilitators," including software providers for peer to peer technology, hackers and others who provide the means or information for engaging in such piracy. US law has dealt differently with each group, based largely on their perceived importance to the continued vitality of the Internet.

Internet Service Providers

Internet Service Providers are generally immune from liability under US law. Under the DMCA, so long as ISP's

are engaged in simply transmitting, storing, caching, or retrieving the pirated work, and do not otherwise control the content of the material in question, the timing or routing of its transmission or the identity of its recipients, they are not liable for copyright infringement based on infringing materials posted or transmitted by unaffiliated third parties. (*See generally* 17 USC §511) In order to qualify for such immunity, the ISP must also remove pirated material from its server and/or block access to such materials upon receipt of the appropriate notice from copyright owners regarding the infringing nature of the material. These "notice and take down" procedures also provide procedures for challenging improper removal demands. (*See generally* 17 USC § 512)

Website Operators

Those website operators who post infringing works are generally liable for direct copyright infringement. If they allow the posting of infringing works by others they may be liable for contributory infringement. (*See Religious Technology Center v. Netcom On-Line Communication Services, Inc.,* 907 F. Supp. 1361 (N.D. Cal. 1995)) As noted above, however, under the DMCA, website operators who merely post third party materials, without more, generally qualify for a safe harbor under Section 511 so long as such website operators comply with the DMCA's notice and takedown procedures in Section 512.

End Users

The downloading of pirated works from the Internet usually qualifies as direct copyright infringement. Such downloading qualifies as an unauthorized reproduction, even if the end user is unaware of the infringing nature of the work. Uploading copyrighted works onto websites and the like similarly qualifies as an unauthorized reproduction of the work. Despite such potential liability, until the RIAA

instituted its aggressive litigation posture in connection with illegal P2P file trading (described briefly above), end users were rarely the focus of civil lawsuits. Such hesitation is not based on a lack of legal basis for a successful suit, since as discussed more completely below, such end users do *not* usually qualify for any fair use defense. Instead, it appears based on the sometimes questionable decision that copyright owners should not sue "potential" customers for their pirate activities. Locating a guilty website owner may also prove difficult since many domain name registries do not require accurate contact information for registrants.

Facilitators

As noted above, 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. The *Sony* doctrine, however, presents a serious limitation to the success of an action against any such distributors.

Briefly in accordance with the Court's decision in *Sony Corp. of America v. Universal City Studios, Inc.*, 464 U.S. 417, 429 (1984), a party is not liable for contributory copyright infringement if such liability is based on the distribution of a staple article of commerce, such as a video cassette recorder used to record broadcast television programs for time-shifting purposes, which has substantial non-infringing uses. Such non-infringing uses include 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. (*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)(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. Thus, for example, in *A&M Records, Inc. v. Napster, Inc.*, 284 F.2d 1091 (9th Cir. 2002), the court ultimately held that Napster's actual knowledge of the infringing nature of its end users' acts vitiated any defense under *Sony*.[12] 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. 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.

Since the *Grokster* case is currently on appeal, it is not yet clear to what extent facilitators who provide software, without more, remain subject to successful legal challenge.

---

[12] *See also In re Aimster Copyright Litigation*, 334 F.3d 643 (7th Cir. 2003).

3. *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, and the ability to settle disputes prior to the institution of a lawsuit will be severely curtailed.

4. *Fair Use*

The law is clear that the unauthorized file trading in copyrighted songs does *not* presently qualify as a fair use. There is presently no "personal use" right to download songs from the Internet or to trade them *unless the copyright owner has consented to such activities.* No categorical fair uses exists for the creation or distribution of copyrighted works on the Internet under US law. In order to determine whether a particular use is "fair," the same statutory analysis applies, regardless of the nature of the use in question. This statutory analysis requires that four non-exclusive factors be considered to determine whether a particular use qualifies as a "fair" one. These four factors are:

1. The purpose and character of use (whether such use is for profit),

2. The nature of the copyrighted work (fiction versus non-fiction),
3. The amount and substantiality of the portion used in relation to the copyrighted work as a whole, and

4. The effect of the use on the potential market for or value of the copyrighted work. (17 USC § 107)

Infringing uses for purposes such as criticism, comment, news reporting, teaching, scholarship, or research are often regarded as fair uses. However, no particular use is considered automatically fair. Consequently, for example, if someone is reproducing portions of another's work for purposes of criticism, the fairness of such uses is still judged using the statutory factors described above. No one factor is determinative. Early cases relied heavily on the market impact of any alleged fair use. (*See Harper & Row, Publishers, Inc. v. Nation Enterprises,* 471 U.S. 539 (1985))

The undeniable adverse market impact on Internet piracy argues strongly against any recognition of a "personal use" right to engage in unauthorized file trading of copyrighted works. At its most fundamental level, any determination that an otherwise infringing act is excused because it is "fair" is in reality the grant of an uncompensated compulsory license. Compulsory licenses are largely disfavored because they remove the right of a copyright owner to control the use of her work. *Uncompensated* compulsory licenses are even more disfavored.

Recently, however, the importance of market impact analysis has diminished so that in some cases transformative uses may trump a copyright owner's rights even when potential adverse market impact is likely. In the seminal case, *Campbell v. Acuff Rose Music, Inc.*, 510 US 569 (1994), the Supreme Court held that the creation of a rap parody of the song "Pretty Woman" qualified as a fair use in light of the transformative nature of the use in question. Even alleged

market impact in the form of reduced potential license fees for rap versions of the original song were considered insufficient to negate a fair use defense.

Although US law does not currently recognize a fair use right to engage in P2P file trading, media transfer rights in certain limited situations have been recognized as legitimate fair uses. Under Section 1008 of the Copyright Act, originally enacted as part of the Audio Home Recording Act, consumers were granted an exemption from copyright infringement for the non-commercial use of a "digital recording device" to make digital or analog musical recordings. [13] (17 U.S.C. §1008) This right was recognized as part of a legislative effort to deal with the challenges to copyrighted works posed by the introduction of digital audio devices, such as DAT. A similar right may well be recognized in the digital environment of the Internet.

In addition to growing debates over the scope of a personal fair use right, free speech concerns have increasingly been raised in copyright cases in the US.

### 6. *Copyright and the First Amendment*

Early fair use cases treated the consideration of fair use as striking an appropriate balance between copyright protection and the free speech concerns of the First Amendment. Thus, in *Harper & Row, Publishers, Inc. v. Nation Enterprises,* 471 U.S. 539 (1985), the Supreme Court recognized that copyright was "intended ... to be the engine of free expression." Any conflict which may have existed between free speech and copyright restrictions was considered resolved through statutory fair use analysis and

---

[13] A digital recording device under the statute by definition includes MP3 players, but not computer hard drives. Thus, the limited media transfer fair use right of the Audio Home Recording Act has no application to the issue of P2P file trading. *See, e.g., A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004 (9th Cir. 2001).

the idea/expression dichotomy. Although First Amendment issues were occasionally raised as a "plus factor" in traditional fair use cases, its presence did not significantly effect the scope of protection afforded copyrighted works.

A sea change occurred with the Eleventh Circuit's decision in *Suntrust Bank v. Houghton Mifflin Company*, 252 F.3d 1165 (11th Cir. 2001). The court overturned the grant of a preliminary injunction in a case involving a purported literary parody of "Gone With the Wind" on the grounds that such injunction qualified as an illegal prior restraint under the First Amendment. The court in its modified decision subsequently backed away from its earlier categorical reliance on the prior restraint doctrine to reject the lower court's grant. (*See SunTrust Bank v. Houghton Mifflin Company*, 268 F.3d 1257 (11th Cir. 2001)) Yet since *SunTrust Bank*, First Amendment defenses have played an increasing role in copyright cases. While such defenses to date have not been wholly successful, it appears clear that copyright enforcement will remain a free speech battle-ground for the near future.

In *Universal City Studios v. Corley*, 273 F.3d 429 (2d Cir. 2001), the defendant's reliance on the First Amendment was ultimately unsuccessful in avoiding liability for violations of the anti-circumvention provisions of the DMCA. Yet despite this failure, the court recognized that software qualifies as protected speech under the First Amendment, making it more likely that a free speech defense may be successful in the future.

More recently, in *DVD Copy Control Association v. Bunner,* 2003 WL 21999000 (Cal. Sup. Ct. 2003), the lower court's refusal to grant a preliminary injunction for trade secret violations involving the unauthorized disclosure of computer software as an unconstitutional prior restraint was overturned on appeal. The court held that the First Amendment "does not prohibit courts from incidentally enjoining speech in

order to protect a legitimate property right." Ultimately, based on the parties' stipulation that the defendant had misappropriated trade secrets, the court found the injunction to be a content neutral prohibition which did *not* qualify as an unlawful prior restraint. Noting that the "special vice of a prior restraint is that communication will be suppressed ... before an adequate determination that it is unprotected by the First Amendment" is made, the court found that the stipulated presence of a trade secret violation sufficient to overcome any free speech defense.

### 7. *Anti-Circumvention Measures*

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)) or to protect "a right of a copyright owner." (17 USC § 1201(b)) 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." (17 USC §§ 1201(a) & (b))

Violations of these anti-circumvention provisions 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 $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. Recidivists penalties are significantly elevated. (*Id.)*

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

1. Non-Profit Libraries, Archives And Educational Institutions;
2. Law Enforcement, Intelligence And Other Government Activities;
3. Reverse Engineering;
4. Encryption Research;
5. Security Testing ; and
6. Protecting Personal Identification Information.

It does not, however, 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 materials to use in teaching activities is not excused from compliance, even if such act would 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) Given the strong lobbying efforts of organizations which represent end users and others opposed to blanket prohibitions against the circumvention of technological protection measures, it seems likely that some form of fair use exemption will ultimately be adopted.

Unless such fair use is available only for personal acts of circumvention, as opposed to the trafficking in circumvention devices (which appears highly unlikely), copyright owners' ability to rely on legal measures to protect their circumvention technologies will be reduced. This reduction will, in my opinion, lead to a subsequent diminution in the effectiveness of such measures, and may ultimately serve as a disincentive to copyright owners to invest in the necessary technology to protect copyrighted works. Ultimately the absence of such protection measures may result in a marked decrease in the amount of published copyrighted works, particularly for collaborative works which require intensive research and/or development monies. With no measures to protect against piracy and assure an acceptable financial return, distributors and creators may be unwilling to invest in the creation/distribution of such cost intensive works.

With the growing demand for an end to circumvention protection has come a reactionary move to self-help measures by copyright owners. "Guerilla tactics," such as running websites that contain free downloads of songs, etc. infected with computer viruses are increasingly discussed as potentially viable methods for combating Internet piracy. More recently, copyright owners sought to expand their self-help rights legislatively through the introduction of HR 5211. HR5211 would grant expanded rights to disable personal files of end users on a publicly accessible, peer to peer file

trading network. Although HR 5211 met serious opposition, and has not been re-introduced, it reflects a hardening of positions on both sides of the copyright enforcement divide. Diverse bills have been introduced into the present session of Congress dealing with the issue of copyright enforcement, including HR 2752 which authorizes $15 million to the Department of Justice for investigation and prosecution of copyright infringement. It is too soon, however, to predict what the ultimate outcome will be.

8. *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:

1. The title or other identifying information, including the information contained on a copyright notice.

2. The name or other identifying information about the author.

3. The name or other identifying information about the copyright owner of the work.

4. 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.

5. 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.

6. The terms and conditions for use of the work (such as licensing contact information).

7. 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. Recidivists 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))

*Potential Solutions to P2P Piracy*

Realistically, solutions to the problem of digital piracy can be briefly categorized into three areas. They are:

1. Business Solutions
2. Technological Solutions
3. Legal Solutions

The choice of which solution(s) may be appropriate in a given business transaction will depend on the subject of the deal, as well as the nature of the work, and the anticipated level and type of pirate activity. In reality, the most successful solutions combine aspects of all three.

*Business Solutions*

*1. Do Nothing*

Like bootleg whiskey during prohibition, some consider digital piracy to be inevitable. Instead of spending business assets combating digital piracy, they contend that such assets

should be used in other more economically fruitful ways. This argument assumes that the costs of any anti-piracy program necessarily outweigh its benefits. While the scope and size of an anti-piracy program, like any other business decision, should be based on a cost-benefit analysis, doing nothing is not a cost-free activity. To the contrary, piracy is like a rock rolling downhill. Without any technological or legal brakes, the rock only rolls down faster. The option of doing nothing may be acceptable where copyrighted assets do not form a substantial product base for a company. It may be economic suicide, however, if the company's major assets consist largely of copyrightable works.

### 2. *Alter the Business Model*

One of the greatest excuses for digital piracy offered by its consumer-practitioners is the high cost of acquiring legitimate products. Quite bluntly, why pay $20 for a music CD, when I can get it for free (and at virtually the same quality) on the Net? It is undeniable that the Internet is the source of problematic pirated copies, but, to state the obvious, it also offers opportunities for developing new distribution methods that take advantage of its economies of scale and access. The SME (Small and Medium Enterprises) development efforts of the World Intellectual Property Organization are only one example of a global recognition of the business opportunities the Net offer. The secret, however, is to develop business models that take advantage of these opportunities, while applying the common sense learning of the bricks and mortar world.

Because of its ability to permit rapid, and relatively inexpensive reproduction and distribution of copyrighted works, the Internet provides a variety of options for combining traditional distribution and marketing techniques with digital technology. Among the types of business models that various copyright industries utilize to combine

traditional techniques and Internet opportunities are the following:

A. Offering works over the Internet for free or markedly reduced prices in order to promote hard goods sales of the works. (Internet Promotion Model)

B. Offering copyrighted works over the Internet through digital ordering or subscription services. (Internet Distribution Model)

C. Creating value-added products in the hard goods world that make pirate versions less desirable. (Value Added Model)

Internet Promotion Model

Under the Internet Promotion Model, web-based versions of copyrighted works may be full length versions of the original, versions which have been tailored to meet the perceived needs or interests of Internet end users, or excerpted copies which provide teaser copies of the original and allow access to full versions only upon payment of a subscription fee. The most common examples of such models arise in the periodic publishing industry. Thus, for example The New York Times website (www.NYTimes.com) offers a modified version of its newspaper while The Economist (www.Economist.com) offers a limited access version of its magazine. Under this limited access model, key articles may only be accessed by payment of a fee-based subscription.

Internet Distribution Model

As opposed to websites such as Amazon.com, which are primarily hard goods ordering sites; many copyright industries are exploring the desirability of developing innovative digital distribution models. Such models include digital subscription services for music, films and software. The development of a workable Internet Distribution Model, however, often raises direct conflicts with traditional hard goods distribution systems. In industries such as music and publishing, bricks and mortar distribution centers are well established and may serve as direct competitors with digital distribution and subscription services. This competitive nexus raises perplexing business issues regarding the inter-relationship between hard goods and cyber-goods, including the extent to which the same products should be offered in both locations and the types of pricing and discount offers that should be developed for each channel of the distribution stream.

One of the legacies of Internet piracy is a growing resistance to paying for copyrighted works that can be obtained relatively easily from pirate sites on the Net. Once customers have become used to free music (for example), it is more difficult to develop a digital subscription service that will meet the demands of these customers, while maintaining acceptable profit levels for content providers. I have conducted several informal surveys among students regarding potential business models for downloadable works. They all indicate that what these consumers desire is: (1) the availability to preview works prior to purchase; (2) an unlimited selection of downloadable works, which includes both current hits and old time favorites; (3) the unlimited right to transfer a downloaded work among media, including computer hard drives, MP3 players and CDs; (4) the right to further distribute the downloaded work, including by sale; and (5) an inexpensive price. To a certain extent the failure

to provide adequate consumer choice in downloadable works, the high price of legitimate CD's, the absence of affordable CD singles, and the limitations on media transfer of authorized downloadable works fueled the growth of illegal P2P file trading in the music industry.

There is strong evidence that a viable Internet distribution service, one that provides adequate access to works at an acceptable price, however, can greatly reduce the scope of illegal P2P file trading. The growth of such services as iTunes, Buymusic and the newly re-launched Napster, and their early success rates,[14] show that a large number of customers will use lawful digital distribution services, particularly when continued infringing activity poses a realistic threat of legal action.

If an e-business solution is to be effective, rights clearance for the Internet must be made easier so that new business models for the public distribution of copyrighted works can be created and offered at prices and terms that make such services desirable.

Despite the potential economic opportunities which digital distribution provides, competitive digital download services have been slow to develop. Part of this delay is due to the entertainment industry's historic failure to embrace new technologies.[15] Some of this historic reluctance is undoubtedly fueled by a desire to control completely the channels of distribution. Another significant contributor,

---

[14] *See, e.g,* Lisa Takeuchi Cullen, "How to Go Legit," Time (September 22, 2003).

[15] *See, e.g,,* Lisa Napoli, "Think Debate on Music Property Rights Began with Napster? Hardly", New York Times (September 24, 2003 (detailing industry's initial failure to embrace such diverse communication media as cassette recorders and MP3 players); John Schwartz, "Music's Struggle with Technology," New York Times (September 22, 2003)(detailing industry's initial failure to embrace such diverse communication media as video cassettes and FM Radio).

however, may be the complicated rights clearance system in place for those who want to provide digital download services for copyrighted works.

As noted above, US copyright owners have the exclusive right to do or authorize the reproduction, adaptation, distribution, public performance and public display of their works. In the case of sound recordings, copyright owners also have the right to perform the work publicly by means of a digital audio transmission. (*See generally* 17 U.S.C.§ 106)

Given these rights, in order to provide the right to download a lawfully copy of a copyrighted sound recording, the service provider must obtain reproduction and distribution rights from the copyright owner of both the musical composition and the lyrics. Because the copy in question will be provided in digital form, the service provider must also obtain the consent of the copyright owner in the sound recording. Thus, there are potentially three different copyright owners whose consent must be obtained before a work can be offered for digital download. Such consent generally takes the form of compensation, complicating the distributor's ability to offer downloads that can compete with the "free" price of illegally file traded copies.

The rights clearance process is further complicated since courts have repeatedly recognized that electronic rights are different from rights in the hard goods world. Recent cases such as the Supreme Court's decision in *New York Times Company, Inc. v. Tasini,* 533 US 483 (2001), demonstrate that digital rights in copyright are often distinct from rights in the hard goods (print) world.[16] Thus, old agreements

---

[16] *See also Random House, Inc. v. Rosetta Books LLC* , 283 F.3d 490 (2d Cir. 2002)( court upholds denial of preliminary relief regarding plaintiff's claim that the publication of books was covered by print agreement, noting the need to examine "the evolving technical processes and uses of an e-book" before adopting any such analogy).

granting the right to publish or distribute copyrighted works in traditional media may *not* be sufficient to grant publishers the right of digital distribution.

Pre-Internet, singers had no right to control the public performance of their works. Consequently, radio stations were only required to compensate the composers for the music they played. Since the Audio Home Recording Act, however, in the case of sound recordings, performers have the right to control the performance of their copyrighted works "by means of digital audio transmission. (17 U.S.C. § 106(6)) This new right is usually not covered in pre-Internet, pre-Napster agreements.

New rights require new agreements, and potentially, additional compensation. The practical effect may be to make it more difficult for service providers to clear the necessary rights for digital distribution. The impact of this differing treatment has already been felt in the area of Internet webcasts, where radio stations that provide simultaneous webcasts must pay additional royalties beyond those already paid for public performance over the airways of the work in questions.[17]

Value Added Products

Finally, in order to combat piracy, some companies are designing hard goods products that have sufficient additional value to make pirated products less desirable. Such additional value may include product based enhancements (such as extended liner notes) or warranty or technical

[17] Public Performance of Sound Recordings: Definition of a Service, 37 CFR Part 201 (providing that FCC licensed radio broadcasts engaged in webcasting are not exempt from copyright liability under the digital performance right, and are subject to the payment of license fees for such webcasts).

support services. To be successful, these value-added attributes must be publicized and must be perceived (or promoted) as commercially desirable for consumers.

*Technological Solutions*

Although technological solutions to Internet piracy remain largely ineffective, business solutions without the necessary technological support to limit unauthorized uses are, in my opinion, unworkable. Unbreakable codes are pipe dreams. But there are many other types of technological solutions that can support legal and business efforts to reduce Internet piracy. Among the most promising are the following:

1. Increasingly sophisticated copy protection and encryption techniques. For every horror story about a copy code that can be circumvented by a magic marker, there are other codes which are helping to reduce illicit copying.

2. Water marking and other digital identification techniques. Even if copy cannot be fully protected against illicit copying, digital identification techniques can provide useful evidence in suits and criminal prosecutions against pirates and other copyright infringers. While many pirates have the know-how to break copy protection technologies, they often pay little attention to digital identification markers. This eases the burden of proof on copyright owners and assists in securing quick temporary restraint measures when illicit websites are located.

3. Copyright Management Information. Similar to digital watermarking, the insertion of copyright management information provides another method for tracking and proving piracy. Furthermore, as noted above, under the DMCA the removal of such

information alone provides a cause of action for preventing the further distribution of pirated works.

Although technology is constantly improving, technology alone can never provide a complete solution to Internet piracy. In an effort to give "teeth" to technological protection measures for preventing the unauthorized distribution of copyrighted works on the Internet, US law currently provides legal protection for such technological measures. These protection measures, contained in the Anti-circumvention provisions of the DMCA (17 USC §1201 et seq, (discussed above)), however, are currently the subject of heated debates. Whether they will survive the current onslaught of fair use activists remains problematic. At present, however, they remain a valuable tool in crafting technological solutions to piracy.

*Legal Solutions*

At the time that the DMCA was enacted, neither Congress nor the lobbyists, I suspect, realized how quickly technology would develop to make present legislative solutions inadequate to solve the piracy problems posed by P2P file trading. The next generation of technology will no doubt see both better file compression and more complex encryption techniques to make the tracking of illegal downloads of copyrighted works even more difficult.

There is no question that the growth of P2P file sharing opportunities has had a harmful impact on those industries whose major economic assets are copyright protected works. In discussing the need to resolve the "conflict" between P2P file trading and the protection of copyrighted works, many have suggested that we must chose whether to protect copyright on the one hand, or privacy and personal use on the other. The impossible choice between intellectual property rights and technological innovation is a phantasm. There is

no such conflict because neither can exist without the other. Copyright serves a critical role in encouraging the creation of new works that enrich the future public domain. As recognized in the US Constitution, copyright protection exists "to promote the progress of science and the useful arts." (US Const. Art. 1, §8. cl.8) Reducing the scope of protection afforded copyrighted works threatens the vitality of the public domain, from which all new creators derive the building blocks for their works. Thus, it is in no one's interest to effectively eliminate copyright protection for works that are traded over the Internet or in other digital formats. Without the building blocks that today's copyrighted works provide for tomorrow's public domain, the scope of future creativity and innovation will undoubtedly suffer.

In addition to encouraging the creation of new creative works, copyright law also encourages their dissemination by providing copyright owners with the exclusive right to control the public distribution of their works. (17 U.S.C. §106(3)) As each new medium of communication has evolved, from cameras, to motion pictures, to the Internet, the entertainment industry eventually recognizes that the new medium provides opportunities for even greater dissemination of its works. Thus, protecting the potential distributive opportunities of P2P and other methods of digital distribution on the Internet is in the interest of society in general and copyright owners in particular.

Nevertheless, with the growing reluctance to hold the creators of P2P software liable for the infringing uses of their end uses, and the recent refusal to allow ministerial subpoenas to be issued against conduit ISP's, the cost of litigation in this area is bound to increase.

*Practical Recommendations*

All copyright protected works should contain a copyright notice so long as such notice does not interfere with the artistic nature of the work. Such copyright notices eliminate innocent infringer defenses, and may also give rise to a cause of action for violation of copyright management information integrity.

Where works exist in digital form, such as software, digital watermarks and other identifying techniques should also be used to help identify pirate products. Such identification measures may help copyright owners track pirated product and also serve an important evidentiary function.

Enforcement responsibilities should be specified in the underlying contract of the applicable business transaction. Among the responsibilities which should be clarified in any such contractual arrangement is who bears the responsibility for any costs incurred for enforcement activities, who decides the parameters of a copyright enforcement program, including the technological and legal steps to take to protect the value of copyright assets, and who has the authority to settle copyright infringement actions.

Not every copyright asset needs to be protected to the fullest extent. To the contrary, businesses should select only those copyright assets which are most important to them and spend enforcement resources on protecting those assets from piracy.

As a practical matter, any enforcement policy should include decisions about the steps that will be pursued against the various categories of pirate activities as a matter of policy. While such policy decisions should remain flexible they will serve a useful purpose in focusing enforcement activities and in budgeting appropriate resources to protect the copyright assets at issue.

Among the categories of potential pirates for which policy decisions should be made are the following:

1. Fan Sites, Slam Sites and Competitor Sites that may use excerpted or derivative versions of original copyright assets.

2. Facilitator Sites that offer free software to assist in the illicit reproduction and/or distribution of categories of copyrighted works that include the major copyright assets of the company.

3. Single owner sites that offer free downloads of pre-release and/or newly released versions of copyright protectable works.

4. End users who engage in P2P file trading, including university and corporate liability for permitting such activities on university/company systems.

Given the international nature of the Internet, domestic enforcement activities may be insufficient to fully protect the copyright assets of the business. While every country is a potential source of pirate activity, for purposes of developing and funding a viable enforcement program, it is preferable to identify those countries which warrant major enforcement focus. Such countries may include major markets or potential markets for copyright assets, or major sources of pirate sites.

Internally, at least one staff member should be required to search the web periodically to locate troublesome sites so

that appropriate action can be taken to take down such sites and prevent the further erosion in value of copyright assets.

To reduce the costs of enforcement activities, companies should become active in industry-based trade associations. Such trade associations often have their own enforcement programs, and can spread the costs of enforcement on an industry wide basis. These programs are particularly important in combating international piracy, where costs can rapidly become prohibitive.

Masters, negatives and other original versions of copyrighted works should be secured through stringent protection measures. Such preventative techniques may at least reduce the possibility of pre-release piracy.

Value added products should be marketed wherever viable. Such value added products make pirated works less attractive because they have a markedly reduced quality.

Companies should not only consider, but also implement, new e-business models for distribution that provide reasonable digital access to copyrighted works. While the presence of such models will not eliminate all pirate sites, they may help reduce their number or frequency.

Digital enforcement programs should be part of, and coordinated with, any hard goods enforcement programs since many of the same concerns raised by digital piracy are raised in the hard goods world.

Copy protection appropriate to the level of exposure of the relevant business assets should be developed and applied. Copyright protection measures are still useful for deterring some people from engaging in Internet piracy and may help to reduce enforcement costs. Among the types of protection

measures that should be considered are technological locks, coded use tools, and encryption.

Copyright management information, including copyright notices, should be included on all publicly distributed copies. While copyright notices are not required under US law, such notices provide a useful method for warning end users that the work they are copying is copyright protected. Moreover, such notices provide useful contact information for end users who wish to obtain a license to utilize the work in question. Finally, for copies which are distributed digitally, copyright management information and other digital markers may assist enforcement personnel in tracking pirate copies, thereby reducing enforcement costs.

Finally, I would recommend that any business that must face the problem of Internet piracy should work closely with local prosecutors to prosecute the most egregious offenders. In cases of international enforcement, companies should keep government agencies, such as the United States Trade Representative and the US Patent and Trademark Office apprised of problems so that bilateral solutions can be achieved. However, whenever companies seek governmental assistance, I would strongly urge them against backing down once the enforcement process has been initiated. Ask yourself whether the prosecutors in the Skylarov case will pursue another piracy case anytime in the near future? Whether or not the prosecution should have been initiated, the only lesson learned was that copyright owners cannot be trusted to stay in the game for the long haul. In an era of exponentially-increasing piracy, that is one message no copyright owner should ever want to send.

*The Future*

As Internet piracy becomes more intractable, I believe that we will see more end user litigation as an enforcement

device. The public relations theory that end users who engage in peer to peer file transfers of copyrighted works are potential customers who should not be sued is difficult to reconcile with the possession of thousands of illegal downloaded files.

I also believe that fair use exceptions for anti-circumvention provisions will be added to current provisions. These fair use exceptions will make technological protection measures less effective. The end result, however, may be to make self help measures, such as the removal by copyright owners of illicit files, more acceptable. Ultimately, privacy concerns may give way to the need for copyright owners to protect their works. One thing is clear, the battle is far from over.