Gartner G2

Copyright and Digital Media in a Post-Napster World

Version 2 (Updated January 2005)

By GartnerG2 and The Berkman Center for Internet & Society at Harvard Law School

Table of contents

0. Introduction

Digital technology and the Internet are altering many industries and changing the way people use and enjoy consumer electronic products, media and entertainment. Although beneficial in many respects, this evolution also exacerbates the tension among copyright holders (individual creators and corporate content providers), technology companies and consumers. This three-way tension is an important driver for business. When balanced, it provides all the benefits of a market-driven economy: Products are created, developed and distributed; and consumers choose from a variety of contents and goods while paying a price they perceive as reasonable. However, when some part of this digital media ecosystem gains a disproportionate measure of influence, the system becomes destabilized. In time, the instability may yield a new equilibrium, but its ultimate effects are difficult to anticipate in the short run.

Technological development spurs change today and, as in other technologically turbulent periods, old methodologies and business models persist as new consumer-behavior models develop. In the case of digital media—music, movies and print—the transition to fully formed digital distribution services is now in progress.

What happens during this transitional period is important on a cultural as well as a commercial level. In the United States, for example, social values such as allowing access to information and creating an environment that encourages development and creation were important considerations in the codification of copyright law in the U.S. Constitution and later statutes. Digital media policy should respect these values as well as producing economic benefit.

The objective of this White Paper is to provide a foundation for evaluating key questions facing copyright holders, technology developers and consumers. These include:

- How do we balance the legitimate interests of copyright holders with the legitimate interests of the public in the use and enjoyment of digital media?
- Should technology developers be accountable to copyright holders?
- What future strategies might compensate copyright holders while also encouraging innovation?

The focus of this White Paper is on the issues confronting U.S. copyright holders and consumers. An International Supplement to this White Paper deals with international legal and regulatory issues.[1]

[1] *Available at http://cyber.law.harvard.edu/media/wpsupplement2005 or http://www.gartnerg2.com/wp/wp-1204-0003.asp*

In this document, initially released in August 2003 and updated in January 2005, the Berkman Center for Internet & Society at Harvard Law School and GartnerG2 explore issues surrounding the current digital media ecosystem including:

- The legal and regulatory developments regarding copyright and related intellectual property issues.
- Business models upset or enabled by digital media distribution.
- Technological developments driving change across the value chain.
- Shifts in consumer attitudes and behavior.

Focusing on these topics, we identify five scenarios that flow from developments in law, technology and society. We describe the five scenarios at the end of this document.[2] They have provided an analytical structure for a series of conferences and recently published papers as well as research in progress. For further information, please visit the Digital Media Project's frequently updated Web site.[3]

[2] *See http://cyber.law.harvard.edu/media/scenarios or http://www.gartnerg2.com/wp/wp-0903-0003.asp.*
[3] *See http://cyber.law.harvard.edu/media/.*

1. Evolution of Copyright Law: How We Got Here

Given the charter of this document, it is logical to start with the foundations of U.S. copyright law and its limitations. In addition, we consider briefly the issues that arise with enforcing copyright law across international borders. Legal and regulatory issues in Europe and Asia/Pacific are discussed in greater detail in the International Supplement to this White Paper.[4]

The U.S. Constitution and the Copyright Act

The U.S. Constitution authorizes Congress to "promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries."[5] This clause is interpreted to direct Congress to strike a balance between encouraging innovation by rewarding authors, and promoting the public interest by allowing for the free use of authors' works at the end of the "limited times."

In the original Copyright Act, Congress granted authors 14 years of exclusive control over their works; over many subsequent amendments, it has extended the term incrementally. In 1998, the most recent revision, the term of copyright increased to life plus 70 years for individual authors and 95 years for corporations.

The U.S. Supreme Court upheld the constitutionality of this most recent extension (see *Eldred v. Ashcroft,* section 3 below). Still, other limitations on the rights of copyright holders to control use and enjoyment of their works remain. With the advent of new technologies such as the personal video recorder (PVR), courts are again weighing the rights of copyright holders against these traditional limitations.

Limitations on copyright

Any work in a "fixed" form with a modicum of originality is eligible for copyright protection.[6] Registering the work with the U.S. Copyright Office provides significant benefits,[7] but is not necessary for protection.[8]

---

[4] *See http://cyber.law.harvard.edu/media/wpsupplement2005.*
[5] *U.S. Const. art. I, § 8, cl. 8.*
[6] *Under the Copyright Act, a work is "fixed" when it is "sufficiently permanent or stable to permit it to be perceived, reproduced or otherwise communicated for a period of more than transitory duration." 17 U.S.C. § 101 (1994). Movies, song recordings and books are obvious examples of fixed works. A live television broadcast is "fixed" if it is recorded simultaneously with the transmission. Id.*
[7] *17 U.S.C. § 411(a) (1994) (preventing authors from suing for copyright infringement unless their work has been registered with the Copyright Office).*
[8] *17 U.S.C. § 102(a) (1994).*

As a result, much of the content on the Web is copyrighted since it is fixed in computer storage and expresses its ideas in some original way. Unless a work is excluded for other reasons, no copyright mark is required. A copyright holder has a number of exclusive rights in an original work: The public cannot copy it, sell it, or make adaptations of it without permission while the work is under copyright protection.[9] However, there are important limitations on the copyright holder's control, including the "first sale" doctrine, the "idea/expression" dichotomy and the doctrine of "fair use."

The **first sale doctrine** provides that certain of the copyright holder's rights end after the first sale of a particular copy of a work.[10] On this basis, a video rental store can rent videos to customers and a library can lend its books without needing permission from the copyright holder or author. This legal concept does not provide a safe harbor in the context of digital media, however, because works shared over the Internet are not simply "borrowed." Instead, in virtually all instances, Internet uses of works make a new copy, thus technically infringing the copyright holder's exclusive rights to reproduce and distribute the work.

The **idea/expression dichotomy** is the legal principle that copyright protection covers the particular expression of an idea, but does not extend to the idea itself.[11] For example, a playwright cannot prevent others from writing a play incorporating stock characters and themes from the playwright's own work, so long as the later writers do not copy the playwright's own expression of those themes.[12]

Fair use of a copyrighted work does not require the creator's permission. Such use includes criticism, commentary, news reporting, teaching, research and certain personal uses. The Copyright Act, however, does not specify which uses are fair, but rather establishes a four-factor balancing test for courts to employ on a case-by-case basis. The four factors[13] are:

- The purpose and character of the use.
- 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 on the potential market for, or value of, the copyrighted work.

---

[9] 17 U.S.C. § 106 sets forth the exclusive rights: (i) to reproduce the copyrighted work in copies or phonorecords; (ii) to prepare derivative works based upon the copyrighted work; (iii) to distribute copies or phonorecords of the copyrighted work to the public by sale or other transfer of ownership, or by rental, lease, or lending; (iv) in the case of literary, musical, dramatic, and choreographic works, pantomimes, and motion pictures and other audiovisual works, to perform the copyrighted work publicly; (v) in the case of literary, musical, dramatic, and choreographic works, pantomimes, and pictorial, graphic, or sculptural works, including the individual images of a motion picture or other audiovisual work, to display the copyrighted work publicly; and (vi) in the case of sound recordings, to perform the copyrighted work publicly by means of a digital audio transmission.

[10] Codified at 17 U.S.C. § 109(a).

[11] See, e.g., Baker v. Selden, 101 U.S. 99 (1879).

[12] See, e.g., Nichols v. Universal Pictures Corp., 45 F.2d 119, 121-22 (2d Cir. 1930).

[13] Codified at 17 U.S.C. § 107. Analyses employed by courts in other jurisdictions will be discussed below.

This last element is critically important in an era of rapidly evolving technology.

Consumers may consider certain uses of copyrighted digital media fair, such as making back-up copies of a DVD. But in many instances, the law is not definitive. Congress has, on a variety of occasions, responded to the confusion with legislation aimed at protecting the rights of copyright holders while also respecting the traditional limitations of copyright.

Statutory responses to digitization

The **Audio Home Recording Act (AHRA)**[14] of 1992 emerged from a compromise between the interests of the recording industry and those of consumers, who were then represented by the Home Recording Rights Coalition. The recording industry's principal concern at the time was preventing the proliferation of consumer electronics devices capable of reproducing sound with perfect quality. The AHRA requires that digital audio recording devices include a system that precludes serial copying (making copies of copies). It establishes a royalty on sales of new digital audio recording devices, payable to the recording industry, and provides a safe harbor for consumers' personal use.

Technology, however, has outstripped the AHRA and made it ineffective as an enforcement mechanism for the recording industry. It has also proven ineffective as a defense for companies that provide file-sharing services to consumers.

A significant problem is that many devices do not fall within the scope of the AHRA. The Act covers "digital audio recording devices," but excludes many common relevant devices.[15] Computer hard drives, for example, have many uses other than storing audio data; therefore, the AHRA does not cover them. Video home recording devices also do not fall within its scope.[16] Other new devices, such as MP3 players, are not included because they are capable only of playing material uploaded to them, rather than of reproducing material on their own.

Companies that provide file-sharing services to consumers have tried unsuccessfully to use in their defense the safe harbor provisions in the AHRA.[17] For example, Napster argued that use of its service constituted noncommercial use of a digital audio recording device; this interpretation would have immunized users and centralized but unmanaged file-sharing services like the original Napster from copyright infringement liability. The court disagreed; accordingly, the AHRA is increasingly irrelevant to legal conflicts involving the digital distribution of music.

---

[14] *Pub. L. No. 102-563, 106 Stat. 4237 (1992).*
[15] *17. U.S.C. § 1008.*
[16] *The U.S. Supreme Court ruled consumer home recording from VCR devices for later playback is protected under the fair use doctrine in Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417 (1984).*
[17] *See In re Aimster Copyright Litig., 252 F. Supp. 2d 634 (N.D. Ill. 2002), aff'd, 334 F.3d 643 (7th Cir. 2003). Aimster took the position that the AHRA shielded Aimster from liability because the AHRA forbids actions based on the non-commercial use of a device to record digital or analog music recordings. 17 U.S.C. § 1008. The court, however, found that Aimster's services involved the copying of MP3 files from one user's hard drive onto the hard drive of another user, and held that this activity did not fall within the AHRA's protections.*

The **Digital Millennium Copyright Act (DMCA)**[18] of 1998 strengthens protections against unauthorized access to copyrighted material and provides an additional layer of legal protection to copyright holders beyond the protections granted by the Copyright Act. The DMCA makes it a crime to circumvent the technological measures that control access to copyrighted works.[19] It also criminalizes the manufacture and distribution of any technology or tool designed to circumvent encryption technology[20]—a strike aimed directly at halting piracy of copyrighted works in a digital format. These restrictions, however, apply even to individuals who create or use a circumvention tool to make a legal or fair use of encrypted material. Although a few narrow exceptions exist, the provisions do not currently exclude users who want to make fair use of copyrighted materials.

Section 512 of the DMCA provides certain safe harbors to online service providers (defined as "a provider of online services or network access, or the operator of facilities thereof"). Internet service providers (ISPs), Web hosting services and search engines all qualify as types of online service providers. These providers are protected from liability for users' infringement if they have a copyright agent to respond to requests by copyright holders to remove infringing materials and follow the Act's procedural requirements. This removal procedure is referred to as "notice and takedown."[21] Still, even if an online service provider does not follow the Act's safe harbor requirements, the provider may not be liable for its users' infringing acts because its role does not meet the legal standards for contributory or vicarious liability.[22] The safe harbor provisions merely provide additional shielding for online service providers.

In addition to proscribing circumvention of access controls and the creation or distribution of tools for such circumvention, the DMCA regulates broadcasts of digital audio transmissions (i.e., by Webcasters and satellite radio stations). Providers of music or other audio content over the Internet fall into two categories: interactive and noninteractive. Interactive digital broadcasters allow listeners to control what they listen to; under the DMCA, they must negotiate directly with individual copyright holders or their representatives (e.g., performing rights societies) for licenses to provide the copyrighted content. Noninteractive broadcasters operate like traditional radio stations and are permitted to operate provided they compensate copyright holders via a statutory license, with a fee periodically set by a Copyright Arbitration Royalty Panel.

---

[18] Pub. L. No. 105-304, 112 Stat. 2863 (1998). See http://www.loc.gov/copyright/legislation/hr2281.pdf.

[19] Section 1201 (a) (1) states "no person shall circumvent a technological measure that effectively controls access" of a copyrighted work.

[20] Sections 1201 (a) (2) and 1201 (b) state that "no person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology" that can circumvent access controls or copy protection technologies.

[21] See http://www.chillingeffects.org/dmca512/notice.cgi?NoticeID=98#FAQID226.

[22] See Metro-Goldwyn-Mayer Studios, Inc. v. Grokster Ltd., 380 F.3d 1154, 1160-66 (9th Cir. 2004). The Grokster decision is further discussed infra, section 3.

Under the DMCA, Web digital radio broadcasters must pay royalties to record labels and recording artists. In contrast, traditional radio broadcasters pay a royalty only to composers, because radio broadcasts are thought to benefit the recording industry through promotional value.[23] One justification for the additional burden on Web radio stations is the claim that digital transmissions are "perfect" copies of songs and their broadcast could therefore facilitate piracy or copying by listeners.

The **No Electronic Theft (NET) Act,**[24] signed into law in December 1997, criminalizes the distribution of pirated software. This Act is another statute enacted to protect copyright holders' interests, although it is rarely invoked. The NET Act imposes liability even on individuals who do not profit from such distribution, closing a loophole that previous laws left open. Similar to the DMCA, the **Computer Fraud and Abuse Act**[25] of 1984 broadly prohibits tampering with or otherwise violating another person's computers or computer systems. This statute has been invoked most notably against search robots and entities sending "spam" e-mail. However, the open-ended statutory prohibitions may be more broadly construed to make illegal copyright holders' self-help measures, such as "spoofing" and "interdiction," against peer-to-peer (P2P) file-sharing of copyrighted material.

In the next section, we discuss the technological developments that drive these changes in copyright and related law, the effect the developments are likely to have on current business models, and concomitant shifts in consumer buying patterns and behavior.

[23] *See http://www.kurthanson.com/archive/news/062002/index.asp.*
[24] *Pub. L. No. 105-147, 111 Stat. 2678 (1997).*
[25] *Pub. L. No. 98-473, ch. XXI, 98 Stat. 2190 (1984) (codified at 18 U.S.C. § 1030); see also http://www4.law.cornell.edu/uscode/18/1030.html.*

2. Business Models in Transition

The emergence of devices that deliver increasingly high-quality reproduction and/or playback of copyrighted digital material—most commonly, music and movies—has driven many of the recent changes in copyright and intellectual property law. Perhaps the most significant development took place in the early 1990s, when CD-ROM drives became commonplace in personal computers, jumpstarting the PC's shift from a pure productivity tool to an entertainment platform. The Internet further complicates matters by facilitating consumers' ability to redistribute content in digital form.

Mass adoption of PCs and VCRs changed consumers' expectations, notably by introducing the notions of time- and location-shifting. It also marked the beginning of the end of the entertainment industry's ability to control the distribution of content by controlling the physical medium on which the entertainment was delivered.

The ability to control how content gets to consumers is a cornerstone of the content industry: music, film, television and publishing companies. Business models in the past century presumed, and reasonably so, the industry's ability to control product distribution through physical channels (e.g., book or record stores) or via controlled broadcast channels (e.g., movie theaters, radio or television). Copyright holders had a straightforward—though not foolproof—way to keep track of their work. Duplicating copyrighted works entailed considerable costs. And before digital technology, illegal copies were generally inferior to the original, thus making piracy arguably less attractive.

What confounds the content industry today is how to shift a century's worth of business models as quickly as digital technology evolves—or at least how to keep within sight of new technologies.

Music

The Internet and PCs equipped with CD-ROMs and CD burners have had a profound impact on the music industry. Traditional revenue streams are based on a complex series of relationships among composers, recording artists, record labels, performance rights organizations, broadcast outlets and retailers. Before the Internet arrived, these relationships worked because the means for producing and distributing content were complex but relatively easy to control given the long history of industry standardization and legal protections. New technologies have undermined this control. With the arrival of the MP3 file format and the popularization of P2P file-sharing through Napster and its progeny, the industry faces further challenges.

Napster terrified the music industry but also illuminated the potential benefits of digital distribution, including the ability to deal directly with an individual consumer without the burden and expense of a physical distribution network. Part of the industry's strategy is now to secure this type of transaction and, in light of KaZaA and other decentralized P2P networks, to create an alternative service more compelling than illegal file-sharing. Success would transform PC and Internet technologies into vital marketing tools for recording artists and the music labels themselves. Labels could use Web sites to promote new releases and provide music samples as well as offer near-instantaneous access to an artist's back catalog.

By mid-2004, two archetypes for legal alternatives to file-sharing sites emerged:

- **À la carte services** sell digital versions of songs as individual tracks. Songs are protected or "wrapped" with digital rights management (DRM) software that controls how the content can be accessed, for example, the number of times they can be copied onto PCs, portable music devices or CDs, or the brands of players on which they can be played. However, once the consumer pays for the content, he owns it permanently.

- **Subscription services** require consumers to pay a monthly fee—in mid-2004 the standard fee was $9.95/month—to access the songs or albums they select via their PCs and play them at will (instead of a radio-like preprogrammed list). After-market devices enable users to stream content to their existing stereo systems located separately from the PC. A limitation of the subscription model is that consumers cannot move the songs onto portable music players.

As the ultimate arbiters, consumers showed a distinct preference for the à la carte model in 2004, with the iTunes Music Store racking up 100 million download sales between its launch in April 2003 and July 2004. The subscription providers—Rhapsody and Napster's premium service—have established audiences but are relatively small by comparison (though from an economic perspective, they deliver more predictable revenue streams to the providers).

Most important, however, all five major record labels and hundreds of smaller, independent labels have made chunks of their catalogs available through these services.

Film

TV (first broadcast, then cable) and the **VCR** provoked the first major shift of the film industry's business model. TV networks and cable outlets became profitable secondary markets for the studios. Although first perceived as a threat, the VCR eventually turned the film industry's business model on its head, with the revenue stream from movie rentals and sales surpassing that from ticket sales.

The arrival of the **DVD** exacerbates an ongoing challenge to the film industry: the threat of "bootlegged" copies of copyrighted films. Bootleg copies can be made from commercially released DVDs or copies of so-called "promo" DVDs distributed for advance screenings. Disney's Buena Vista Home Entertainment division offers an alternative: DVDs that render themselves unplayable 48 hours after rental, using technology from Flexplay Technologies.

The **Internet** is proving to be the most disruptive force the movie industry has faced. Distributing films over the Internet is increasingly easy, either through Web sites like Movie88.com or via P2P file-sharing networks. Credible estimates of the financial impact of Internet movie piracy are hard to find. Former Motion Picture Association of America (MPAA) president Jack Valenti cited Viant, a Boston-based consulting firm, for the estimate that 400,000 to 600,000 movies are illegally downloaded daily.[26]

While the movie industry experiments with solutions to battle both mechanical copying of DVDs and online piracy, it is also testing ways to get movie content online in authorized—and thus controlled—fashion. In mid-2002, industry members banded together to launch Movielink.com, a joint project of MGM Studios, Paramount Pictures, Sony Pictures Entertainment, Universal Studios and Warner Bros. (A competing service, Intertainer, is currently offline due to an ongoing legal battle with the major studios; Intertainer alleges it abandoned its support of the service in favor of Movielink.)

Movielink allows users with a broadband PC connection to purchase temporary access to films at roughly the same time they become available at video rental stores. The digital content is stored on the user's PC's hard drive; the purchaser may view the film as many times as desired within a 24-hour period starting at the first viewing. The user has 30 days to access the film from the time of purchase. When either the 24-hour or 30-day period ends—whichever comes first—the Movielink client erases the content from the hard drive.

Another company that provides film viewing on demand is CinemaNow, which uses a proprietary distribution and DRM technology platform to protect content. Launched in June 2001, CinemaNow has not published official subscriber numbers but claims at least 1 million unique visitors each month. Both of these services are still new and their chances for long-term success are difficult to gauge.

STARZ Ticket on Real Networks launched a third alternative form of online movie distribution in June 2004. Aimed at on-the-go consumers, STARZ Ticket allows consumers (for a monthly fee) to download movies from STARZ's current selection onto as many as three PCs. Consumers can watch the movies as often as they want for as long as the movie remains available on the STARZ service.

---

[26] *See http://www.mpaa.org/jack/2003/2003_02_24.htm.*

Television

Advertising dominates TV's traditional revenue model. Cable TV simply introduced a new revenue stream from subscribers. In recent years, other revenue streams have emerged: selling boxed sets of a season's worth of popular shows like "The X-Files," "Sex and the City" and "The Sopranos," and selling shows into syndication.

The TV industry remained relatively stable throughout the Internet explosion of the 1990s. It is only with the more recent introduction of the **PVR** that the traditional advertising-dependent revenue model has come under serious threat.

The two leading PVRs, ReplayTV and TiVo, allow viewers to set preferences for recording programs and subject matter, to watch programs they have previously selected whenever they choose and to fast-forward through commercials. ReplayTV used to allow viewers to skip commercials entirely, but the feature was cut[27] following former owner SonicBlue's bankruptcy and the sale of ReplayTV to D&M Holdings, a Japanese holding company that owns the Denon and Marantz brand names. However, users can still fast-forward in 30-second increments, a standard length for a television commercial. The conflict between broadcasters' need to sell advertising and viewers' desire to skip it will be further exacerbated as Microsoft's Media Center PCs (and similar offerings such as the open-source Freevo Project) extend PVR-like functionality to PCs and similar features are incorporated into the next generation of set-top boxes deployed by cable and satellite TV companies. The network capabilities of TiVo, ReplayTV and the cable companies' set-top boxes, however, are already engendering new targeted advertising opportunities that signal one possible evolution of the revenue model.

The effect of these technologies may be to significantly alter the concept of "prime time" TV viewing. Indeed, PVRs could undermine virtually every TV advertising tactic and strategy developed in the past 50 years. In an apparent reaction to such concerns, TiVo executives in November 2004 announced that the company developed an advertising service that allows advertisers to create ads that will pop-up on screen while a user fast-forwards through commercials embedded in a broadcast.

Publishing

Books were once typically sold through retail stores, with "book-of-the-month" clubs adding revenue via catalog sales. Online retailers such as Amazon.com pioneered a new retail channel but did not alter the fundamental business model. The media remains analog and thus copyright is not any more imperiled than in traditional bricks-and-mortar retailing.

Digitized online versions of print publications—magazines and newspapers—and "e-books" are another matter, because of the possibility of digital piracy. Yet this risk is of little concern to the

[27] *See http://www.siliconvalley.com/mld/siliconvalley/6062475.htm?template=contentModules/printstory.jsp.*

industry. Incremental ad revenue is a financial incentive for print publications to launch online versions, but the primary source of consumer revenue remains subscription and newsstand sales. Advertising, however, is the primary revenue source for physical newspapers and magazines. Meanwhile, consumers have not embraced e-books, most likely because the digital reading experience neither adequately replicates nor improves upon the analog reading experience.

Some still see promise for the online subscription model. *The Wall Street Journal* has always required a separate paid subscription for its online version, and *Consumer Reports* is reportedly the first online publication to attract 1 million subscribers. But virtually every newspaper that launched a Web site in the past four years gave visitors free access, so convincing consumers to pay for online content is difficult.

As for e-books, the ElcomSoft case may be an illustration of smoke without fire or flame. ElcomSoft's Dmitry Sklyarov created a pirate's tool before there was any substantial content available and worth stealing. E-book titles have not yet approached the number or richness of their paper counterparts—and indeed, may never do so if consumers continue to show little interest in them.

Changing consumer behavior

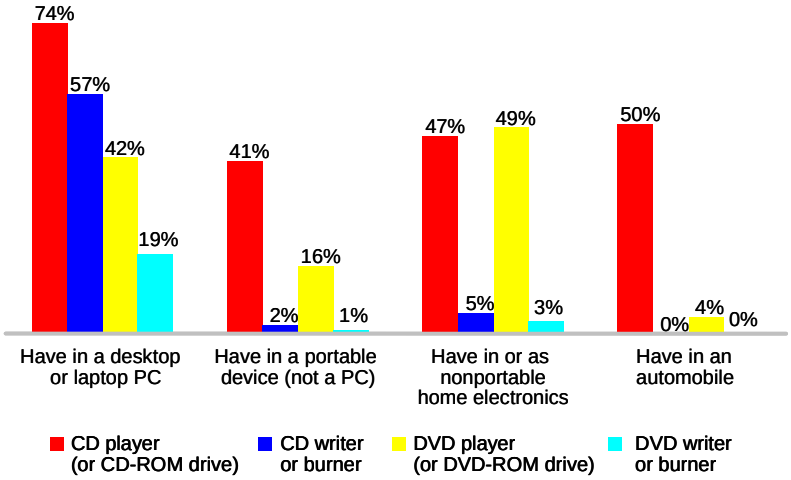
New technologies disrupt existing business models, but only to the extent the public embraces them. By late 2001, PC manufacturers and consumer electronics companies provided consumers with the technology to store vast quantities of digital content on massive hard drives, and with the software necessary to create digital copies of prerecorded CDs.

By the fall of 2004, 18 million consumers were copying CDs and 27 million consumers were making CDs from music files stored on their PCs, according to a survey of online adults by GartnerG2 conducted in September 2004.[28] This relatively regular copying of digital media is not unexpected given high levels of ownership of digital copying technologies. As illustrated in Figure 1, 60% of online households reported owning a CD-writer/burner in a PC, while 21% of these households reported having a DVD-writer/burner in a PC, according to a GartnerG2 survey of online Americans.[29]

[28] *Respondents included 2,540 adults aged 18 or older. GartnerG2 selected samples to be representative of online individuals with respect to geography, market size, household income, household size, and presence of children. The adult sample was also selected to be representative of online individuals with respect to age.*

[29] *The survey was completed by respondents at 2,455 U.S. households in June 2004 with samples chosen to be representative of online households with respect to geography, market size, and income.*

Figure 1: U.S. digital playback and copying in online households



Source: GartnerG2, June 2004

The continual enhancement of the PC platform at ever-decreasing prices has driven the rapid proliferation of these devices. To illustrate, Table 1 shows a Gartner projection of the basic component configuration and prices in 1997 and 2006 for PCs targeted at the mid-range market segment, 20% to 30% of the total market shipments at any time.

Table 1: Breakdown for mid-range PCs

	1997	2006
Hard drive storage	3.2GB	180GB
Optical storage	CD-ROM	DVD-CD-RW combo drive
CPU	Pentium	Pentium
Average selling price	$1,100–$1,400	$1,489

Source: Gartner Dataquest, April 2003

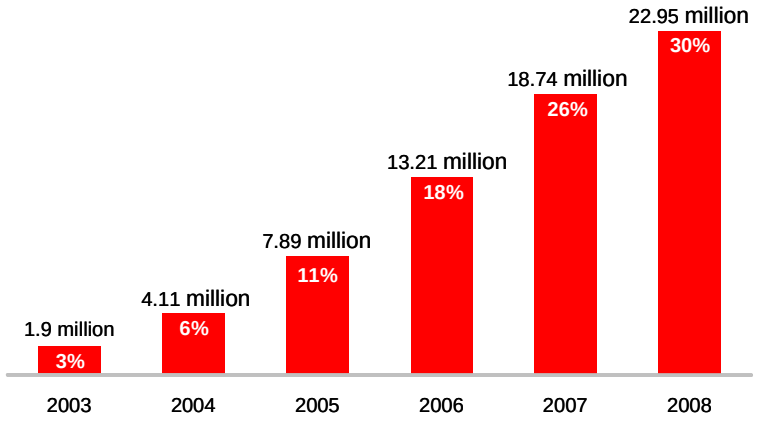
The underlying driver of the PC technology revolution is that functionality increases while end-user prices remain flat or decline. This price-performance progression is fixed in the consumer's mind and has arguably created an important set of expectations: With a mid-range PC and an Internet connection, virtually any type of digital content is available.

Current behavior and future possibilities

As discussed above, the technology base for the digital transition is in place, thanks to the relentless innovation of consumer electronics and PC companies. Consumer behavior is just starting to catch up; the biggest jump remains for consumers to shift the majority of their media purchases from physical media (CDs, DVDs, newspapers, books) to digital files. Ever-larger hard drives will contribute to the move to digital-dominated (or exclusive) media libraries.

However, in 2004, the transition of the music industry was still more about early adopters' experimentation than about broad-scale deployment. Figure 2 illustrates GartnerG2's estimate that in 2004, 6% of U.S. households subscribed to or purchased à la carte downloads from a legitimate music site.

Figure 2: Percentage and total number of U.S. households subscribing to online music or using à la carte services, 2003–2008



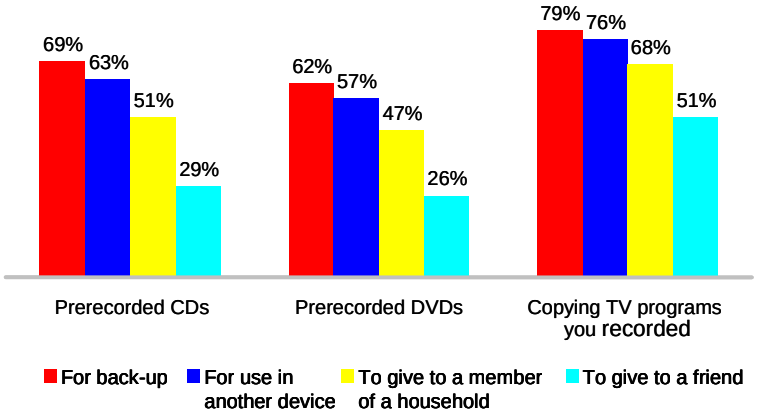
Source: GartnerG2, April 2004

Consumption, copying and sharing

Consumer use of digital media is growing, and one aspect of this use is significant copying for personal use and for sharing with friends. Use of online file-sharing programs is fairly well established for some consumers, but is still not widespread.

U.S. consumers view media, including digital media, as a household resource rather than an individual one. When asked in a GartnerG2 survey of U.S. consumers in October 2003, whether they believed it is legal to make copies of digital content for personal use, back-up or to share with a member of their household, the vast majority of consumers replied that they thought it is legal (see Figure 3). Obviously, most consumers believe their purchase reflects ownership of more than the music's format—they expect to have some degree of "portability" with their digital media files.

Figure 3: Consumer attitudes about copying by media type



Source: GartnerG2, October 2003

Yet consumers also express an inherent understanding of the limitations of fair use, if not a comprehensive knowledge of where the boundary lies between fair use and copyright violation. When asked if they thought it was legal to make a copy of prerecorded content to give to a friend, the vast majority said they believed this was illegal. (The only media format that consumers believed was legal to make copies of and distribute to friends outside of the home is TV content.)

PC technology meets the modern network

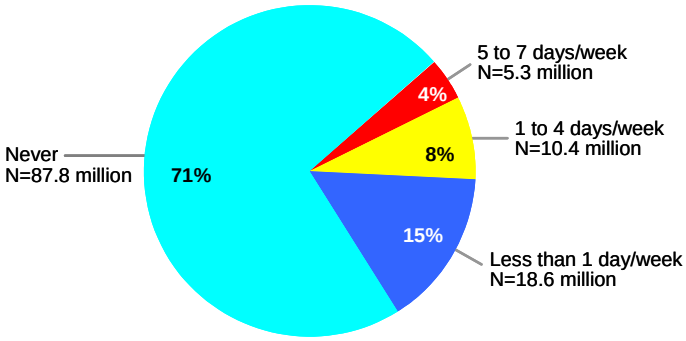
When the price-performance curve of the PC meets up with the Internet and modern networking technology, a truly empowered consumer is born. The popularity of P2P file-sharing in 2000 and 2001 was a wake-up call to the music industry, which recognized that it was losing the ability to control its future through control of physical product distribution. As bandwidth to homes and offices grew through the mid-1990s and into 2002, the perception grew that P2P networks represented a serious threat.

With the fall of Napster, attention focused on more decentralized P2P networks, which maintain no central Web site or server. As discussed in section 3, this difference in the design of decentralized file-sharing software may make such networks less vulnerable to legal challenge.

Gnutella, released in March 1999 by Nullsoft, was the progenitor of these decentralized networks. With the Gnutella protocol, users connect to each other and search requests passed from one user to another throughout the network. No company owns Gnutella, although many people have created programs to interface with the network. Individuals can choose to use the service anonymously through a masked ID. Unlike Napster, Gnutella would be very difficult, if not impossible, to shut down. While popular, the user experience with these P2P network clients—the client resides on the consumer's PC—is far from easy. Users have to learn how to use the system, and locating and downloading content can take a few minutes or hours, depending on the content.

Much hype and rhetoric surrounds the issue of file-sharing sites, and in mid-2004 there were conflicting studies about the financial effects of file-sharing on the music and movie industries. In fact, the MPAA has placed a disclaimer on its Web site noting that its current piracy estimates do not include Internet-based file-sharing. A robust file-sharing community exists worldwide—according to Download.com, by 1 August 2004, more than 124 million copies of the Morpheus file-sharing client had been downloaded, along with 77 million copies of the iMesh client. However, downloads do not necessarily equate to use, and a GartnerG2 survey of U.S.-based Internet users conducted in September 2004 paints a somewhat more restrained picture of file-sharing services (see Figure 4).

Figure 4: Consumer use of file-trading sites (self-reported)



Source: GartnerG2, September 2004

While the number of respondents using file-sharing services is substantial and most likely growing—more than 18 million adults 18 years and above admitted using file-sharing sites "less than once a week" (as opposed to "never"), and an additional 5 million adults stated they use file-trading sites five to seven days per week—responses would indicate that these users are in the minority. The conflict between the numbers of downloads and of admitted traders of files likely results at least in part from respondents' self-serving answers due to the **Recording Industry Association of America's** (RIAA) legal actions against consumers who share files. As noted in Figure 4, the most popular response among respondents in all categories was "never and not interested" when asked about plans for using file-sharing sites to obtain music.

'Legitimate' P2P and 'legal' sharing

A group of new applications and new service providers aiming to leverage two core capabilities of P2P networks—the ability to browse an enormous catalog of music and, increasingly, movies and the ability to share this content with others—emerged near the end of 2004. These new applications or services can be categorized thusly:

- **"Legitimate" P2P.** These services include Wippit and Weed. These systems are built on aspects and

structures similar to decentralized P2P networks. The big difference is that instead of unlicensed copyrighted material being traded, the content is seeded in the networks by rights holders. Weed, from Shared Music Licensing, Inc., allows users to find songs, listen to the complete song three times before having to pay for it (typically through a PayPal account). At that point, users can share the songs by passing them along to others. The second set of consumers then has the same choices as the first consumer. Rights holders receive compensation from the initial purchase transaction and each subsequent transaction. In a nod to the importance of the music fan's role in promoting and raising awareness of their favorite bands and to encourage them to use a legitimate service, the Weed system actually pays users who pass along music that other users purchase in turn. (For each transaction, the rights holder gets 50%.) The transaction chain goes back three generations of sharing. The proceeds from the first sale, before a subsequent "chain" of fans is developed, go back to the independent content provider (e.g., a music distributor, aggregator or manager). Weed's system supports WMA-based files and WindowsDRM. A related service comes from PassAlong Networks, which has licensed content from the major labels. The PassAlong system is based on the same notion of letting consumers legally share playlists of song clips via e-mail or instant-messaging clients. The receiver can sample the songs and then follow the links to the PassAlong store, where they can purchase the content. Those who share music with others receive loyalty points that they can use to purchase songs.

- **"Legal" sharing.** Examples of such services include Grouper and Mercora. Though they differ in their specific approach to consumers and the elements of copyright law upon which they build their offerings, they share a common strategic thrust: enabling consumers to package and present their libraries of music. Grouper allows users to create lists of visitors to go online, listen to playlists, and view digital pictures and digital videos. The key is that the services stream content rather than offering it for copying and downloading. Also, Grouper's model limits the number of people to 30, including the group leader, who can participate in a listening group. The company believes this equates to a private performance, exempting them from Internet radio broadcaster status. The potential benefit for the music industry is that these listening rooms can become new promotional channels while also serving as a legal-sharing alternative to the existing P2P networks.

As these new forms of legal sharing were introduced in the last half of 2004, the music industry also made moves toward using the existing P2P networks as legitimate distribution channels. Shawn Fanning, developer of the original Napster technology,

co-founded SNOCAP, a technology company that garnered a lot of press attention at the end of 2004. SNOCAP is a set of technologies which includes a “content identification system” based on technology licensed from Philips Royal Labs. SNOCAP’s systems will comb existing P2P networks—the appropriate technology is embedded in a P2P software client—identify and index songs. The database will then be available to license holders such as music labels, which can then apply any business rule, such as wrapping the content in DRM that specifies the number of times a piece of content can be copied. Once indexed and tagged, these files then flow throughout a P2P network. However, rather than simply downloading and copying, users would have to adhere to whatever rules the rights holder had created. Observers expect that P2P services that utilize SNOCAP will not allow “free” sharing side-by-side with the licensed content.

These developments lead to the conclusion that while their illicit P2P usage could continue to increase, a significant number of consumers are not interested at this point in using the P2P networks exclusively, and forms of legal sharing are becoming available. The message to music companies and movie studios is that, among those citizens interested in accessing digital media online, a significant number are likely open to a legal alternative to illegal P2P sites, and these new alternatives can be important allies in the music industry’s drive to fashion profitable business models in the digital era.

3. Relevant Cases and Developments

Recently, the copyright industry's lawsuits against file-sharing networks such as Napster, KaZaA and Grokster, and the legal campaign against individual file-sharers, have gained much public attention.[30] In this section, we take a broader perspective and consider the legal cases and decisions that form the background for today's conflicts over copyright and digital media under relevant U.S. case, statutory and constitutional law.[31] We group cases under five headings:

- Copyright and the U.S. Constitution
- Fair use and digital technology
- Enforcing the DMCA
- Electronic publishing rights
- Beyond copyright (other laws used to protect creative control or distribution)

And finally, a separate section discusses international enforcement issues from the U.S. perspective.

Copyright and the U.S. Constitution

In ***Eldred v. Ashcroft***,[32] the Supreme Court affirmed the constitutionality of the Sonny Bono Copyright Term Extension Act of 1998 (CTEA) as well as, some argue, Congress's right to continually extend copyrights. The case arose when online publisher Eric Eldred, who put public domain works online when copyright terms expired, found that the CTEA placed works he intended to publish on the Web outside the public domain for another 20 years.

Eldred argued that the CTEA violates the Constitution's "limited times" clause, citing nearly a dozen previous legislative extensions of copyright terms and the First Amendment. The Supreme Court disagreed, ruling that the CTEA's 20-year extension of copyright is technically a "limited time." Furthermore, the Court stated that examining the policy implications of such extensions is a matter for Congress and that heightened First Amendment scrutiny should be

---

[30] The Recording Industry Association of America (RIAA)—supported by actions of the U.S. Department of Justice --has sued more than 7,704 American music file-sharers since August 2003. See, e.g., http://www.siliconvalley.com/mld/siliconvalley/news/editorial/10433480.htm. Recently, the Motion Picture Association of America (MPAA) filed its first round of lawsuits against alleged file-traders, see http://www.wired.com/news/digiwood/0,1412,65730,00.html. MPAA has also taken actions against operators of websites that had served as hubs for file-sharing networks such as BitTorrent. See, e.g., http://news.com.com/BitTorrent+file-swapping+networks+face+crisis/2100-1025_3-5498326.html?tag=nefd.lede.

[31] For a discussion of foreign laws, see the International Supplement to this White paper, at http://cyber.law.harvard.edu/media/wpsupplement2005.

[32] 537 U.S. 186 (2003). See http://www.supremecourtus.gov/opinions/02pdf/01-618.pdf.

pursued only when "Congress has…altered the traditional contours of copyright."[33]

The decision may hinder future court challenges to copyright law, as *Eldred* sets a strong precedent for judicial restraint in copyright cases. At the same time, it may be possible for future challengers in fair use cases to argue that a particular law—the DMCA, for example—alters copyright's "traditional contours," because the Court implied that fair use is critical to balancing copyright with the First Amendment.[34]

Fair use and digital technology

Decided by the Supreme Court in 1984, ***Sony Corp. v. Universal City Studios***[35]—also known as the *Betamax* case—remains the benchmark for determining whether purveyors of consumer technologies that enable infringement can be held liable for users' illegal acts. The Court found that Sony's VCR was "capable of substantial non-infringing uses" that fell under the Copyright Act's fair use exceptions and therefore Sony could not be held liable for users' copyright infringements. Specifically, the Court determined that time-shifting copyrighted TV programming for later personal, noncommercial viewing constituted fair use under the Copyright Act. Although the "substantial non-infringing use" standard for fair use has since protected other manufacturers from liability, the DMCA may now limit its application in situations where copyright holders use technology to protect their content. Several tests of fair use with more recent technological developments are discussed below.

In ***RIAA v. Diamond Multimedia Systems***,[36] the Ninth Circuit Court of Appeals determined that making a device that enables portable playback of digital music files does not equate to contributory copyright infringement, even though users might have pirated the files they played on the device. The RIAA argued that the Diamond Rio portable MP3 player made by Diamond Multimedia Systems encouraged piracy, but the Ninth Circuit agreed with the defendants that that was the wrong test for liability. Specifically, the court stated: "The Rio merely makes copies in order to render portable, or 'space-shift,' those files that already reside on a user's hard drive."[37] The AHRA protects "the right of consumers to make analog or digital audio recordings of copyrighted music for their private, noncommercial use,"[38] and the Diamond Rio enabled that protected activity and thus was legal, despite its concurrent ability to enable piracy.

At the time, many heralded the case as a digital *Betamax*, with the implication that it would shield manufacturers of digital devices that enable users to exercise fair use rights regardless of the potential for unlawful uses. It was also relied upon by

[33] *Id. At 191 (Supreme Court majority opinion).*
[34] *See discussion at http://balkin.blogspot.com/2003_01_12_balkin_archive.html#87596430.*
[35] *464 U.S. 417 (1984).*
[36] *180 F.3d 1072 (9th Cir. 1999).*
[37] *Id.; see also http://laws.lp.findlaw.com/9th/9856727.html (9th Cir. opinion).*
[38] *Id. at 1079.*

emerging companies that distributed MP3 music files over the Internet, including eMusic and MusicMatch.

Distributors of P2P file-sharing software

New Internet-based technologies have tested the boundaries of the Betamax defense, "capable of substantial non-infringing uses." In 2000, the Ninth Circuit found Napster, the first popular Internet file-sharing service, liable for contributory and vicarious copyright infringement, rejecting the company's defense of "substantial non-infringing uses." Napster operated a centralized database indexing all the files available for download on its users' computers. In ***A&M Records v. Napster***,[39] the court held that regardless of whether users could employ the centralized file-sharing system's non-infringing uses, Napster's actual knowledge of the infringing activity, and its material contribution to infringement by its ongoing provision of the site and central indexing services for illegally trading copyrighted files, constituted a basis for contributory liability. The court found Napster's ability to "control" and supervise use, failure to "purge" infringing uses and financial benefit from infringing activity, were further grounds for vicarious liability.

The decision did not sound the death knell for all P2P file-sharing systems, however. In ***MGM v. Grokster,***[40] the court considered a case brought against several other P2P services. Unlike Napster's service, the software developed by the *Grokster* defendants did not create a centralized database of files available for download. Rather, Grokster's P2P users connected and uploaded their file lists to "SuperNodes"—computers with fast connections belonging to users on the network. Although the entertainment-industry plaintiffs argued that distributing software to enable P2P sharing of content, much of it copyrighted, was *Napster* all over again, both the trial and appeals courts agreed with the defendant software companies that the technological distinctions between their services and Napster's compelled a contrary conclusion.

The courts found key elements of contributory and vicarious liability missing. Contributory liability requires the defendant have knowledge of the infringement and make a material contribution to it; vicarious liability exists where the defendant has a financial interest in the infringement and has the ability to control users' activities. Due to the decentralized design of defendants' software, however, the courts found that the services could continue even if the companies shut down. For that reason, defendants lacked control over users sufficient to warrant vicarious liability for users' copyright infringement.[41]

---

[39] 239 F.3d.at 1017 (9th Cir. 2001). For further analysis, see http://www.eff.org/IP/P2P/Napster/20010226_rgross_nap_essay.html; see also http://news.findlaw.com/legalnews/lit/napster.

[40] 259 F.Supp.2d 1029 (C.D. Cal. 2003), aff'd, 380 F.3d 1154 (9th Cir. 2004). Twenty-eight of the largest music and entertainment companies had sued Grokster, StreamCast Networks, and Sharman Networks for operating the P2P file-sharing services Grokster, Morpheus, and KaZaA, respectively.

[41] The parties obviously disagree on the issue of control, among others. KaZaA demonstrated some degree of control when it shut Morpheus out of its network in March 2002, forcing users to upgrade to a new version of KaZaA to continue using the service; see http://news.com.com/2100-1023-851330.html.

The court also held that defendants' software was "capable of substantial non-infringing uses" regardless of whether much of the actual use of the software is infringing. Moreover, the court held that the copyright holders failed to demonstrate that the defendants had reasonable knowledge of *specific* infringing files on their users' computers. Further, it concluded that the defendants did not materially contribute to direct infringements, and, based on the decentralized nature of the network, did not have the ability to "police" the network and block access to individual users.

The entertainment industry has filed a petition for certiorari with the U.S. Supreme Court on 8 October 2004, and the Court later announced it would hear the case. Oral hearings will be held on 29 March 2005.[42] Evidently, the exact implications of *Grokster*—also with regard to other programs that are capable of file-sharing, such as AOL Instant Messenger and Microsoft Outlook—will become clearer after the U.S. Supreme Court's ruling. In the wake of the District Court's ruling, the RIAA filed thousands of lawsuits against individual file-sharers[43] and launched another series of lawsuits a few days after the Ninth Circuit's affirmation.[44]

Despite (or because of) the published decisions in *Napster* and, more recently, in *Grokster*, the legal battle against P2P software distributors continues. Immediately following its success in *Napster*, the RIAA sought and won a preliminary injunction in ***RIAA v. Madster (formerly Aimster)*** [45] in an Illinois federal court. Madster's service enabled AOL Instant Messenger users to share music files over the Internet. Although Madster worked to come up with an effective means to block infringing uses, the Court nevertheless ordered the service to shut down in December 2002.

In its appeal, Madster claimed a "substantial non-infringing uses" defense and tried to distinguish its service from Napster's. [46] However, the Seventh Circuit Court of Appeals affirmed the ruling against Madster.[47] Significantly, the Court framed the *Sony* test to weigh infringing and non-infringing uses, along with the possible cost of redesigning the technology. Such a test differs from the bright-line "capable of substantial non-infringing uses" test of *Grokster* and *Betamax,* and focus of those decisions on the technology providers' ability to control user activity. Although the Supreme Court declined to hear an appeal in the *Madster* case, these conflicting interpretations of *Betamax* could influence the Court to grant certiorari in *Grokster*.

---

[42] *http://www.eff.org/news/archives/2005_01.php#002221.*
[43] *See http://news.com.com/2100-1027_3-5160262.html?part=rss&tag=feed&subj=news; see also http://news.com.com/'Pirate%20Act'%20raises%20civil%20rights%20concerns/2100-1027_3-5220480.html?tag=nefd.lede. See also Sony Music Entm't v. Does 1-40, infra.*
[44] *See http://www.technewsworld.com/story/36149.html.*
[45] *See http://news.com.com/2100-1023-956644.html.*
[46] *See the appeal at http://www.musicpundit.com/download/Aimster%20Appeal%20ReplyBrief_1.pdf.*
[47] *In re Aimster Copyright Litig., 334 F.3d 643 (7th Cir. 2003), cert. denied, 124 S.Ct. 1069 (2004).*

One way the technology sector has responded to the questionable legality of file-sharing has been to create song sharing functionality within legitimate digital music stores. Online music provider MusicMatch, for example, recently added a feature to its service allowing customers to share three plays of a song with noncustomers.[48] Mercora, by contrast, allows users to stream music to others as if they were Webcasters.[49]

Recording television signals

The ability of digital video recorders (DVRs)—also called PVRs—such as TiVo and ReplayTV, to record, store and potentially disseminate TV programs raises important new questions implicating fair use.[50]

In ***Paramount v. ReplayTV*** and **Newmark *v. Turner Broadcasting System,*** consolidated cases that were never adjudicated on the merits, DVR makers and consumers argued fair use to defend against copyright infringement liability. In the first case, a group of major entertainment industry players sued ReplayTV owner SonicBlue in October 2001, arguing that skipping commercials and downloading copyrighted programming constitutes infringement, and that the ability to make and share digital copies of TV programs facilitates piracy. In June 2002, the Electronic Frontier Foundation (EFF) helped a group of ReplayTV users countersue the studios to secure a declaratory judgment that personal use of ReplayTV technology is legal. This included consumers in the debate for the first time. The consumers argued that ReplayTV is similar to the VCR and that ReplayTV's "commercial advance" and "send-show" features were fair uses under the 1976 Copyright Act and the *Betamax* ruling. The cases were never adjudicated due to SonicBlue's bankruptcy and D&M's purchase of ReplayTV.[51]

Enforcing the DMCA

Anti-circumvention provisions

The DMCA protects the interests of copyright holders by prohibiting a range of activities related to breaking access and copy-protection technology ("copy-locks"), and distributing technology that can break such technological protection measures.

---

[48] *See http://news.findlaw.com/ap/ht/1700/7-28-2004/20040728053004_22.html.*
[49] *Id.*
[50] *DVRs can record and store many hours of TV programs directly onto a hard drive. With the right technology and a good Internet connection, DVR recordings can be transferred to a computer and then sent to others over the Internet. Most DVRs record commercials, but during playback users can fast-forward through them, or in the case of older ReplayTV models, skip commercials entirely. The DVR movement is currently undergoing major shifts. Comcast is rolling out a DVR-capable set-top box (STB) in the northeast. See http://www.comcastnw.com/digital_video.htm; http://broadband.motorola.com/dvr/dct6208.asp. PC products, too, are beginning to incorporate DVR functionality. Microsoft's Windows Media Center PC is one such product. See http://www.microsoft.com/windowsxp/mediacenter/default.mspx. The effect of these products on the market for pure DVRs may be significant. Certainly, the willingness of companies to build DVR functionality into other products indicates that the legal waters are now conducive to allowing consumer use of such products.*
[51] *See http://www.siliconvalley.com/mld/siliconvalley/6062475.htm?template=contentModules/printstory.jsp. The second case, Newmark v. Turner, was dismissed as moot in light of the dismissal of the first action. See http://www.eff.org/legal/cases/Newmark_v_Turner/20040109_Order.pdf.*

In ***Universal Studios v. Reimerdes***,[52] the Second Circuit Court of Appeals affirmed the constitutionality of the DMCA's anti-trafficking provision and rejected a fair use defense on these facts: In 1999, Norwegian teenager Jon Johansen cracked the content scramble system (CSS), the principal DVD encryption format. Johansen's stated goal in creating his program, DeCSS, was to provide the means to play DVDs on Linux computers, which did not have a CSS-licensed player. The MPAA member organizations sued *Web site 2600 Magazine* for publishing and linking to DeCSS, claiming that publishing the code was a violation of the DMCA's ban on distributing technology that breaks digital locks on copyrighted content. The defendants claimed that DeCSS has substantial fair uses and that the First Amendment protects the publication of and linking to the DeCSS code. A U.S. District Court and the Second Circuit held that, although the DeCSS computer code is protected under the First Amendment, the DMCA's anti-trafficking provision does not violate the First Amendment. Several similar cases concluded with the same result.

The entertainment industry won another victory in January 2000 with a finding by a U.S. District Court that Streambox's "Ripper" and "VCR program," which defeated RealNetwork's proprietary encryption and control technologies to enable use with non-Real software, conversion into non-Real formats and permanent copying, was likely to violate the access and anti-circumvention provisions of the DMCA. In ***RealNetworks v. Streambox,***[53] RealNetworks obtained an injunction against Streambox's distribution of the Streambox VCR program and on 8 September 2000, the two parties settled.[54] Streambox agreed not to distribute the VCR program or the Streambox Ripper.

As a result of the DMCA, very different rules apply to digital media than to media in other formats. Although in some instances a person can legally tape songs broadcast on the radio, recording digitally streamed media is a different story. A threatened suit by Live365 forced the creator of the open source program Streamripper X, for example, to disable its recording features for the Internet radio Web site Live365.com.[55]

Two District Court rulings against DVD-copying software maker 321 Studios bolstered the entertainment industry's interpretation of the DMCA. In April 2002, 321 launched a pre-emptive strike against the MPAA in California; ***321 Studios v. MGM***[56] sought a declaratory judgment that 321 could continue to promote its DVD Copy Plus software product, which allows users to make (arguably) reduced-quality backup copies of DVDs on CDs.[57] Later that year, 321 included in its complaint its latest product, DVD X Copy, which makes perfect copies of DVDs. The suit

---

[52] *Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2nd Cir. 2001); see http://laws.lp.findlaw.com/2nd/009185.html. See also discussion above at pg. 10.*
[53] *See http://www.law.uh.edu/faculty/cjoyce/copyright/release10/Real.html.*
[54] *See http://news.com.com/2100-1023-245482.html?legacy=cnet.*
[55] *See http://www.chillingeffects.org/anticircumvention/notice.cgi?NoticeID=83; see also http://streamripper.sourceforge.net/index.php.*
[56] *321 Studios v. MGM Studios, Inc., 307 F. Supp. 2d 1085 (N.D. Cal. 2004).*
[57] *See http://www.321studios.com/PR_complaint.html.*

questioned the DMCA's constitutionality and claimed that the First Amendment and fair use protected the sale of both products. The company also argued that the products were geared toward personal, limited copying—not toward piracy—and that the products did not violate the DMCA. The court disagreed and enjoined 321 from manufacturing or distributing its products. A New York District Court arrived at a similar conclusion.[58] Most recently, Atari, Electronic Arts and Vivendi Universal filed lawsuits against 321 Studios, requesting the court to ban sales of 321's Games X Copy utility. Soon afterwards, 321 Studios filed bankruptcy in order to fend off these and other lawsuits in the United States and abroad.[59] Emboldened, the entertainment industry has filed suits against other companies, including Tritton Technologies, QOJ, World Reach and Proto Ventures, which distribute software capable of copying DVDs.[60]

In ***U.S. v. ElcomSoft,***[61] the U.S. government brought criminal charges first against Russian programmer Dmitry Sklyarov and then his employer ElcomSoft for violation of the DMCA's anti-circumvention provisions (see also above). Sklyarov was arrested while attending a U.S. conference to present a paper on a program that disabled the encryption on Adobe's eBook files. The program, called the Advanced eBook Processor, allows people to convert Adobe eBooks to Adobe PDF files, thus circumventing eBook's usage and copy controls—controls that arguably restrict the user's fair use rights unlawfully.[62] As in *Reimerdes*, the government argued that the program posed the risk of facilitating piracy, while the defendants argued that the software enabled fair uses otherwise precluded by eBook's usage and copy controls. ElcomSoft lost a motion to dismiss the criminal case on the grounds that the DMCA's ban was unconstitutional and that the eBook Reader permitted Adobe and the publisher to exert excessive control over the eBook, overriding consumers' first sale and fair use rights. However, a federal grand jury ultimately acquitted ElcomSoft, ruling that the prosecution had failed to prove the requisite mental state for criminal culpability.[63]

Felten v. RIAA bounded the reach of the DMCA with respect to scholarly cryptology research. In November 2000, Princeton University computer science professor Edward Felten defeated the encryption scheme created by the Secure Digital Music Initiative (SDMI), a group of companies seeking to develop a new digital security standard for music. SDMI had invited researchers and hackers to try to crack the technology and offered a reward for their success. When Felten and his team opted to publish their results rather than receive the reward, the

---

[58] *Paramount Pictures Corp. v. 321 Studios, 2004 WL 402756, NO. 03-CV-8970 (S.D.N.Y. 2004)*
[59] *See http://www.321studios.com/ and http://www.pcworld.com/news/article/0,aid,117314,00.asp*
[60] *See http://www.ipjustice.org/091803.shtml.*
[61] *See http://www.eff.org/IP/DMCA/U.S._v_Elcomsoft/.*
[62] *Using AEBPR, users can copy eBooks onto other personal devices, make back-up copies, and excerpt parts of books for legitimate uses. Just like DeCSS, AEBPR helps people using alternative operating systems like Linux, as Adobe's eBook Reader only works on Macs and computers running Windows. See additional examples at http://www.eff.org/IP/DMCA/U.S._v_Elcomsoft/us_v_elcomsoft_faq.html#HowDoesElcomSoftWork.*
[63] *See http://news.com.com/2102-1023-978176.html.*

RIAA threatened to sue, claiming that the research paper constituted a "circumvention device" in violation of the DMCA.[64]

Instead, Professor Felten and a group of fellow researchers, with help from the EFF, filed suit against the RIAA, SDMI and the U.S. government on 6 June 2001, seeking a judicial declaration that the First Amendment protected Felten's right to discuss and publish his work.[65] The RIAA backed off and said it would "never again" threaten Felten, since scientists attempting to study access control technologies are not subject to the DMCA. The case was dismissed in November 2002, as District Judge Garrett E. Brown told the researcher plaintiffs they had no "real case or controversy" with which to challenge the statute.[66] Rather than appeal, the researchers dropped the case, citing the RIAA's promises that they would "never again" challenge such cryptologic research.[67]

The next prominent case involving interpretation of the DMCA's anti-circumvention provisions may arise from RealNetworks' **Harmony**, a piece of software introduced in August 2004 that converts songs from Real's music store (Helix-ACC format) into Apple's FairPlay format, and enables users to play Real's songs on Apple's iPod.[68] A series of complex and fact-dependent questions, such as whether Harmony has to be qualified as a circumvention device, must be resolved to determine whether Real has violated access control technology and, therefore, the DMCA while creating Harmony, or whether RealNetworks' actions—providing for the interoperability of music files—places it within the "reverse engineering" safe harbor of the DMCA.[69]

In this context, we must mention another case—involving garage door openers rather than music stores. In ***Chamberlain v. Skylink***,[70] the Federal Circuit Court of Appeals upheld the District Court's summary judgment, which held that Chamberlain, a maker of garage door openers, cannot use the DMCA to stop a competitor, Skylink, from making remote controls that also work for Chamberlain garage door openers. At the core of this complex decision was the question of what the Congress intended when it passed the DMCA, and how exactly to balance divergent interests in order to fit the equilibrium copyright embodies.[71] Two aspects of the ruling are particularly relevant in the present context. First, the Court held that devices whose only significant uses are non-infringing cannot violate the DMCA. Second, the Court established a test that examines whether a tool or circumvention has a reasonable connection to a copyright granted by the Copyright Act. The reasonable relationship between the circumvention and a use must be demonstrated by the copyright owner who seeks to impose liability on an alleged trafficker. In other words, a copyright owner must demonstrate

---

[64] *See Frequently Asked Questions About Felten v. RIAA, at http://www.eff.org/IP/DMCA/Felten_v_RIAA/faq_felten.html.*
[65] *See http://www.eff.org/IP/DMCA/Felten_v_RIAA/faq_felten.html.*
[66] *See http://www.eff.org/legal/cases/Felten_v_RIAA/20011128_hearing_transcript.html.*
[67] *See http://www.eff.org/IP/DMCA/Felten_v_RIAA/20020206_eff_felten_pr.html.*
[68] *See http://news.com.com/2100-1041_3-5288378.html.*
[69] *17 U.S.C. § 1201(f).*
[70] *381 F. 3d 1178 (C.A. Fed. 2004), see http://laws.lp.findlaw.com/fed/041118.html.*
[71] *See, e.g., http://blogs.law.harvard.edu/cmusings/2004/09/06, http://www.freedom-to-tinker.com/archives/000673.html, and http://blogs.law.harvard.edu/cmusings/2004/09/06.*

that the trafficker's tool enables either copyright infringement or a prohibited circumvention.[72] It has been argued elsewhere that this test might have an impact on the above-mentioned controversy about Real's Harmony (assuming that FairPlay was circumvented), since a court would analyze whether Real's circumvention was reasonably related to a right of a copyright holder. Following this line of reasoning, Real would likely have a strong case, given that the sole purpose of the circumvention was to create Harmony.[73] However, it remains to be seen how courts will apply the test in the future.

In ***Blizzard v. BNETD***[74] (formerly known as *Davidson & Assoc. v. Internet Gateway*), for instance, a District Court of Missouri found that a group of open source developers that reverse engineered a game by Blizzard to enable people to run their own servers to host multiplayer versions of the games conducted an illegal circumvention under the DMCA and violated the relevant end-user licensing agreement.[75] The District Court decision has been appealed, in part based on the *Skylink* rationale.[76]

A limiting effect on the DMCA of different kind might arise from the ruling ***Lexmark v. Static Control***,[77] where the U.S. Court of Appeals for the Sixth Circuit overturned a District Court's order that barred Static Control from making and selling computer chips for ink cartridge replacements. Static Controls reverse engineered Lexmark's authentication procedure between Lexmark printers and toner cartridges to enable refilled and remanufactured cartridges to work on Lexmark products. Lexmark sued, claiming both copyright infringement and circumvention in violation of the DMCA. Before the District Court, Lexmark successfully argued that it would likely succeed on its DMCA claims. The Sixth Circuit, by contrast, stated that this was erroneous and made clear that companies like Lexmark cannot use the DMCA in conjunction with copyright law to create monopolies of manufactured goods for themselves. The decision remanded the case for further proceedings.

ISPs and the subpoena process

ISPs are a new target for the entertainment industry, and the case of ***RIAA v. Verizon*** broke new ground. In August 2002, RIAA asked a federal court to compel Verizon Communications to reveal the name of a Verizon Internet access customer accused of illegal file-trading through the KaZaA network.[78] The DMCA offers an expedited process for subpoenas, such as the one the RIAA procured and served on Verizon, which dispenses with the need to first file a copyright infringement lawsuit. This expedited process requires that, upon presentation of the subpoena, an ISP must identify the alleged infringer to the complaining party.

---

[72] *See http://blogs.law.harvard.edu/cmusings/2004/09/06.*
[73] *See http://blogs.law.harvard.edu/cmusings/2004/09/06.*
[74] *334 F.Supp.2d 1164 (E.D.Mo. 2004), see http://www.freedom-to-tinker.com/doc/2004/bnetd_30sep.pdf.*
[75] *See, e.g., http://www.corante.com/importance/archives/026273.php for more details.*
[76] *See http://www.eff.org/IP/Emulation/Blizzard_v_bnetd/.*
[77] *387 F.3d 522 (C.A.6 2004), see http://lawgeek.typepad.com/04a0364p-06.pdf.*
[78] *See Music body presses anti-piracy case, at http://news.com.com/2100-1023-954658.html.*

Verizon fought back. It did not question the RIAA's right to obtain the customer's identity, but argued that formal legal proceedings are required before a customer's identity can be released under Article III of the First Amendment to the U.S. Constitution. Verizon also claimed that it is only a conduit of information and does not "control or operate" the service, and so the DMCA subpoena process did not apply.[79] A Federal Court disagreed and ordered Verizon to comply with the order, calling Verizon's reading of the DMCA's subpoena and safe harbor provisions "strained."[80] The U.S. Court of Appeals for the D.C. Circuit reversed.[81] It held that because Verizon was not storing the infringing audio files on its servers but was merely acting as a conduit for data exchange between users, the DMCA's expedited subpoena provision did not apply. By agreeing with Verizon's interpretation of the DMCA, the Court did not need to reach the question of the subpoena's constitutionality. In May 2004, the RIAA petitioned the U.S. Supreme Court to review the D.C. Circuit's decision,[82] but the Supreme Court denied certiorari.

The *Verizon* case could indicate a trend toward more restrictive interpretations of the DMCA's provisions; its effects will be felt most immediately in similar lawsuits between the RIAA and ISPs. One such case, filed by *Pacific Bell Internet Services* (now *SBC*), challenges (as did *Verizon*) the applicability of the expedited subpoena provision for pursuing file-sharers and the provision's constitutionality as it applies to ISPs merely acting as a "conduit."[83] Originally filed in California, the case was transferred[84] to the District of Columbia, the same district where *Verizon* was decided. The value of *Verizon* as binding precedent there will hamper the RIAA's attempt to defend its statutory interpretation of the DMCA, if not its defense of the constitutionality question.[85]

Even if courts do not uphold the DMCA's expedited subpoena process, copyright holders will still be able to file individual "John Doe" lawsuits against file-sharers. According to a 2004 Federal District Court ruling in ***Sony Music Entertainment v. Does 1-40***,[86] the file-sharer's ISP can then be compelled to divulge its customer's identity.[87] The Court noted there are First Amendment considerations that must be balanced because file-sharing can constitute free speech. However, in the case before the Court, the copyright holders overcame the hurdle posed by the First Amendment.

---

[79] *See http://www.eff.org/Cases/RIAA_v_Verizon/20030121-riaa-v-verizon-order.pdf Order at 6.*
[80] *In re Verizon Internet Servs., Inc., 240 F.Supp.2d 24 (D.D.C. 2003). See http://news.com.com/2100-1023-981449.html; see also http://www.eff.org/Cases/RIAA_v_Verizon/20030121-riaa-v-verizon-order.pdf.*
[81] *Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Servs., Inc., 351 F.3d 1229 (D.C. Cir. 2003). See also http://news.com.com/2100-1027-5129687.html?tag=nefd_hed.*
[82] *See http://www.eff.org/legal/cases/RIAA_v_Verizon/20040524_Verizon_RIAA_Cert_Petition_Final.pdf.*
[83] *SBC challenges the provision's constitutionality under Article III and the First and Fifth Amendments of the U.S. Constitution. See Complaint for Declaratory Relief, available at http://www.eff.org/IP/P2P/PacBell_v_RIAA.pdf.*
[84] *Pacific Bell Internet Servs. v. Recording Indus. Ass'n of Am., Inc., No. C03-3560 SI, 2003 WL 22862662 (N.D. Cal. 2003).*
[85] *See http://news.com.com/SBC+raps+RIAA+subpoenas+in+court/2100-1027_3-5110775.html?tag=nl; see also http://techdirt.com/articles/20031201/2021213.shtml.*
[86] *2004 WL 1656538 (S.D.N.Y. 2004).*
[87] *See http://news.zdnet.co.uk/business/legal/0,39020651,39161898,00.htm.*

Recently, a U.S. District Court in Pennsylvania issued an order concerning a copyright infringement action entitled ***Elektra Entertainment Group Inc. v. Does 1-6***,[88] which requires that before revealing "John Doe's" information, a subpoenaed ISP must first submit a Court-directed notice regarding issuance of a subpoena to "John Doe." The notice explains to "John Doe" what has happened, how he or she may contest the charges, and grants a period of 21 days to file a motion to quash or vacate the subpoena. During this period, the name of "John Doe" remains undisclosed. This decision seeks to balance plaintiff's enforcement interests on the one hand with due process and privacy rights of the defendants on the other hand.[89]

Copyright holders may also employ traditional legal theories such as copyright infringement directly against ISPs where DMCA-based causes of action fail. However, this approach failed recently in ***CoStar Group, Inc. v. LoopNet***,[90] in which a copyright owner of commercial real estate photographs sued ISP LoopNet for allowing its customers to post infringing photos on the LoopNet Web site. LoopNet had a practice of reviewing photos to ensure both that they portrayed real estate and to verify that the image itself contained no explicit statement of ownership that would be violated by a posting. The Fourth Circuit, affirming the District Court, held that copyright law requires "some aspect of volition and meaningful causation," and that LoopNet's cursory review of users' images did not pass this test for infringement. The court relied on pre-DMCA case law[91] to decide the issue, rejecting the argument that the DMCA codified the relevant aspects of copyright law. The result is a clear statement of the limitations of the DMCA's scope, holding that "'[t]he DMCA did not simply rewrite copyright law for the online world.'"[92]

Electronic publishing rights

In ***New York Times v. Tasini***,[93] the Supreme Court held that periodical publishers do not have the right to license and republish articles in electronic databases such as Lexis/Nexis without the author's permission. Electronic rights, at least in the State of New York, must expressly be included in the publisher's contract with the author (in particular, for freelancers who are not employees of the publication). If the contract does not specify a right to publish in the new format, the publisher does not have that right.

Following the *Tasini* decision, a federal court held in ***Random House v. Rosetta Books***[94] that the publisher's exclusive right to publish and sell the work "in book form" did not give the publisher the right to distribute the work as an e-book. Rosetta Books published e-book versions of literary classics that Random House and others published in physical form;

---

[88] *See http://www.eff.org/IP/P2P/RIAA_v_ThePeople/20041012_Order_Granting_Request.pdf.*
[89] *See http://practice.findlaw.com/cyberlaw-1204.html.*
[90] *373 F.3d 544 (4th Cir. 2004).*
[91] *See Religious Tech. Ctr. v. Netcom Online Communications Servs., Inc., 907 F.Supp. 1361 (N.D.Cal.1995).*
[92] *Id. at 553 (quoting Ellison v. Robertson, 357 F.3d 1072, 1077 (9th Cir. 2004)).*
[93] *533 U.S. 483 (2001).*
[94] *283 F.3d 490 (2nd Cir. 2002).*

Random House subsequently sued. Random House lost the initial court decision but the parties later settled, forging a mutually agreeable licensing arrangement.

The likely effect of these decisions is that the publishing industry will now routinely demand blanket assignment of rights when negotiating the initial contracts with writers and freelancers, thus precluding later litigation over electronic publishing rights.

Beyond copyright

There are numerous legal vehicles for enforcing creative control rights outside of copyright law, such as entering into a contract or seeking trade secret protection. These means can be used defensively or proactively.

While many consumers look to fair use to protect their use of copyrighted content, it is increasingly common for them to waive such rights by contract. In ***Bowers v. Baystate Technologies***,[95] the Court of Appeals for the Federal Circuit affirmed a lower court's ruling that the Copyright Act does not pre-empt contract law and therefore that parties may contractually agree to waive any rights they choose—even fair use protections. Specifically, in *Bowers*, the provisions of a "shrink-wrap" license agreement that prohibited reverse engineering were enforceable.[96]

Bowers follows the line of reasoning in ***ProCD* v. *Zeidenberg***, [97] which held that copyright law does not pre-empt a patent holder's shrink-wrap license. In *ProCD*, the Court said: "A copyright is a right against the world. Contracts, by contrast, generally affect only their parties; strangers may do as they please, so contracts do not create 'exclusive rights.'"[98]

Another development outside copyright enforcement is the claim that certain disclosures, such as posting decryption code on the Internet, unlawfully reveal a company's trade secrets. While *Universal v. Reimerdes* dealt with circumvention technologies pertaining to copyright, the *Pavlovich* and *Bunner* cases addressed trade secret law. Unauthorized sharing of trade secrets may be unlawful, regardless of whether the information shared is copyrighted. The DVD Copy Control Association (DVD CCA), the group that manages CSS licensing, sued several people who published DeCSS online, alleging divulgence of a trade secret (***DVD CCA v. Pavlovich*; *DVD CCA v. Bunner, et al.***).[99] The DVD CCA did not invoke the DMCA in these cases. Instead, it relied upon law protecting trade secrets. The outcomes could have significant effect on the legal landscape, irrespective of any future changes to the DMCA.

---

[95] *320 F.3d 1317 (Fed. Cir. 2003).*
[96] *The Blizzard court (mentioned above) followed and reaffirmed Bowers. The District Court decision has been appealed, and the 8th Circuit Court of Appeals is expected to determine whether the three software programmers who created the open source BNETD game server violated (beside the DMCA) Blizzard's end user license agreement (EULA), see http://www.eff.org/IP/Emulation/Blizzard_v_bnetd/.*
[97] *86 F.3d 1447 (7th Cir. 1996).*
[98] *Id. at 1454.*
[99] *DVD Copy Control Ass'n v. Bunner, 75 P.3d 1 (Cal. 2003); Pavlovich v. Superior Court, 58 P.3d 2 (Cal. 2002).*

It may be illegal to publish information regarding the circumvention of DRM technology if that technology is found to be a trade secret, a standard that is governed by state rather than federal law. In *Bunner*, the California Supreme Court held that code such as DeCSS is not protected speech under the First Amendment for purposes of defeating an injunction if that code is derived from trade secrets.[100] The Court remanded the case to the lower court, however, to determine whether the information revealed by DeCSS could still be considered a trade secret in light of its ubiquitous publication. On 27 February 2004, a California Appeals Court found that CSS was indeed no longer a trade secret.[101]

A similar case, *Pavlovich*, involved an important interstate jurisdictional question. As with *Bunner*, the DVD CCA sued Texas resident Matthew Pavlovich under a trade secret theory for posting DeCSS code; Pavovich partially controlled the Web site containing the posting. The DVD CCA attempted to have Pavlovich tried in California, but Pavlovich argued that California lacked personal jurisdiction over him because he did not intend to interact with or do business within the state of California.[102] The California Supreme Court agreed, holding that Pavlovich's Web posting did not demonstrate that he intended to cause harm in California, and that he had not benefited from the laws of California sufficiently to be forced to defend a lawsuit there.[103]

Online video-on-demand services allow consumers to download or stream licensed media content such as feature-length films. To date, allegations of online movie piracy have been limited, yet so too has access to legitimate film content over the Internet. One such service alleges that this scarcity reflects illegal conduct. In ***Intertainer v. AOL Time Warner***, filed in September 2002 with a trial date set for early 2005, video-on-demand provider Intertainer is accusing five major Hollywood studios of antitrust violations that give studio-backed service Movielink a market advantage (see above).[104] Intertainer has also filed a lawsuit against the studio-backed service Movielink. Intertainer shut down its service in October 2002, purportedly to focus on the lawsuit.[105]

Movielink allows consumers to download full-length movies from the Internet, with full authorization from content providers. The movies provided by Movielink are made available for a limited time and the technology prevents users from copying files, transferring them to another computer or viewing them on another platform.[106] Some fair use advocates argue that Movielink's service is overly restrictive. However, the service is in such an early stage that it is difficult to draw conclusions about

---

[100] *DVD Copy Control Ass'n v. Bunner, 75 P.3d 1 (Cal. 2003); see http://www.cnn.com/2003/LAW/09/04/findlaw.analysis.hilden.dvd/.*
[101] *DVD Copy Control Ass'n Inc. v. Bunner, 116 Cal.App.4th 241 (Cal.App. 6 Dist. Feb 27, 2004)*
[102] *See http://www.eff.org/IP/DVDCCA_case/20020115_eff_pr.html; see also http://www.eff.org/effector/HTML/effect15.27.html#II.*
[103] *Pavlovich v. Superior Court, 58 P.3d 2 (Cal. 2002).*
[104] *See 3 Movie Studios Hit With VoD Lawsuit, at http://ecommerce.internet.com/news/news/article/0,,10375_1469311,00.html.*
[105] *See Film Site Halts Service Pending Lawsuit, at http://news.com.com/2100-1023-962463.html.*
[106] *See Movielink's downloads take time, but they are totally legal, at http://www.usatoday.com/tech/news/techinnovations/2002-11-11-movielink-works_x.htm.*

how it will develop. Currently, the service requires customers to watch full-length films on their PCs, an unusual format in and of itself. Competitive online services are also available, including CinemaNow.

On-demand streaming of audio content took an important step recently with the conclusion of a $1.7 billion **licensing agreement for radio Webcasting** between the American Society of Composers, Authors and Publishers (ASCAP) licensing agency and the Radio Music License Committee.[107] The licensing arrangement essentially ratifies the common industry practice of simultaneous transmission of programming over the radio and via the Web.

International enforcement issues

The Internet has a global reach, while most laws that apply to conflicts over copyright and related rights are still local in nature.[108] From a legal and enforcement perspective, the tension between the global reach of the Internet and local laws raises three analytically distinct questions.

- **Jurisdictional questions.** The problem arises of where lawsuits can be filed and will be heard by courts.
- **The choice-of-law problem**. The question is up for discussion what laws the competent court will apply to a given conflict with connections to more than one jurisdiction.
- **Enforcement problems.** The ability to enforce national rights against foreign entities is often disputed in cross-border disputes.

The following paragraphs illustrate some of the complicated jurisdictional questions and choice-of-law problems.

Jurisdictional questions

The global and long-term availability of content on the Internet raises questions of where lawsuits about such content can be filed and heard. Courts are struggling to balance plaintiffs' potential to experience harm everywhere the Internet reaches with the potentially chilling impact of defendants' potential liability under varying local laws worldwide.

In early 2000, the MPAA filed suit against iCraveTV (***MPAA v. iCraveTV***), a Canadian company, for streaming U.S. and Canadian television programming online without the permission of the U.S. copyright holders.[109] At issue was whether iCraveTV, whose activities were legal under Canadian law, was subject to a U.S. court's authority for violations of U.S. copyright law. A U.S.

[107] *See http://www.ascap.com/press/2004/mlc_101804.html.*
[108] *The International Supplement to this White Paper discusses the tension between global Internet and local laws in greater detail, and provides an overview of the laws and treaties (such as the Berne Convention or the World Intellectual Property Copyright Treaty) that already apply internationally.*
[109] *See iCraveTV is Served Up a Lawsuit, at http://www.wired.com/news/business/0,1367,33797,00.html.*

federal judge granted a temporary restraining order,[110] but the ultimate question was not conclusively answered because iCraveTV shut down its services, citing legal pressures and costs.

More recently, in ***Dow Jones* v. *Gutnick,***[111] Australia's High Court found that U.S.-based publisher Dow Jones & Co. could be sued in an Australian court for defamation it published in an article on the Internet. Dow Jones had argued that proper jurisdiction for the suit was where the servers hosting the article were located—New Jersey in the United States. The High Court disagreed, stating, "It is where [a person] downloads the material that the damage to reputation may be done. Ordinarily then, that will be the place where the tort of defamation is committed."[112]

In January 2004, in ***Bangoura v. The Washington Post et al.,***[113] a Canadian court granted jurisdiction to a suit alleging an American newspaper defamed the plaintiff in articles initially published online seven years earlier. The plaintiff, who had been stationed by the United Nations in Kenya at the time of the articles' publication but had resided in Ontario for the two years prior to the suit, sued *The Washington Post* in an Ontario court, arguing that the articles remained available on the newspaper's Web site and therefore accessible to readers in Ontario. The defendants argued in response that there was no real and substantial connection between the defendants and Ontario, and thus the Ontario court should not take jurisdiction. The court, however, ruled that the defendants should have reasonably foreseen that the story would follow the plaintiff wherever he resided.

If other courts and countries follow the *Dow Jones* and *Bangoura* approach, the impact could be profound. If publishers risk liability in every jurisdiction where their online publications may be accessed or where a plaintiff may reside (even years later), to be safe from suit they would have to ensure that their publications either met the requirements of every jurisdiction's specific laws (leaving a far narrower range of content available) or could not be accessed from some locations (limiting what individuals in those places could reach).

Choice-of-law problems

The international component is one of the more interesting aspects of the U.S. recording industry's suit against P2P network operator **KaZaA**. KaZaA was established in the Netherlands, but then sold to Sharman Networks, a company incorporated on the South Pacific island of Vanuatu and managed in Australia.[114] On 22 March 2002, a Dutch court ruled that KaZaA was not liable for copyright infringement by its users under Dutch law.[115] The Dutch Supreme Court, finally, confirmed the lower court's

[110] *See Broadcasters win battle against iCraveTV.com, at http://news.com.com/2100-1033-236255.html.*
[111] *See http://www.austlii.edu.au/au/cases/cth/high_ct/2002/56.html.*
[112] *Id.*
[113] *See http://www.canlii.org/on/cas/onsc/2004/2004onsc10181.html.*
[114] *See http://www.wired.com/wired/archive/11.02/kazaa.html.*
[115] *See http://news.com.com/2100-1023-870396.html.*

findings (see below).[116] Ten months later, Sharman Networks, now owner of KaZaA, was sued by the recording industry in U.S. courts for allegedly violating U.S. copyright law.[117] In February 2004, the Australian anti-piracy body Music Industry Piracy Investigations initiated copyright infringement proceedings under Australian law against Sharman Networks before an Australian federal court.[118] The uncertainty about jurisdictions as well as differences in the applicable laws—which, in fact, might lead to divergent outcomes—illustrate the enforcement obstacles for U.S. plaintiffs and raise questions about the reach of U.S. law with regard to foreign entities.

With regard to the litigation in the United States, it is noteworthy that other distributors of file-sharing software were recently handed a victory in *MGM v. Grokster* (see below).[119] However, the decision did not vindicate KaZaA; the company did not participate in the suit, perhaps to bolster its (unsuccessful) argument that it should not be subject to U.S. jurisdiction. After the Ninth Circuit's affirmative ruling, Sharman Networks' U.S. counsel announced that Sharman Networks will be filing a motion for summary judgment nearly identical to the successful motions filed by Grokster and Morpheus.[120] However, it is not expected that the U.S. ruling will have a significant impact on the pending case before the Australian courts.[121]

In nations that do not recognize U.S. copyright law, do not have laws similar to the DMCA or are unlikely to enforce U.S. decisions, copyright enforcement may rely on unofficial channels of communication and nuanced interpretation of relevant local law. In 2001, a Taiwanese Web site called **Movie88.com** offered videos on demand for US$1 per three-day "rental." Movie88.com was a few steps ahead of Hollywood in providing such a service; today Movielink and CinemaNow offer comparable services. Movie88.com claimed it conformed to Taiwanese copyright law since it did not make movies available within 30 days of their release. Taiwan's Justice Department, alerted by the American Institute in Taipei as to the company's activities, relied on a different interpretation of the law and closed the site down.[122]

Conflicting national copyright regimes and diverging enforcement practices can lead to another set of international issues, for instance in cases where a person undertakes an activity that is lawful in his country of residence but travels to a nation-state that forbids the activity in question. This particular aspect of the Internet's global reach is illustrated by the case where the U.S. government brought criminal charges against a Russian programmer named Dmitry Sklyarov and his employer, **ElcomSoft** for conduct that took place in Russia and allegedly violated the DMCA (see also above). While working for ElcomSoft, Sklyarov

---

[116] *See http://www.ecommercetimes.com/story/32461.html.*
[117] *See http://news.com.com/2100-1023-980274.html. The court found that KaZaA did meet the "minimum contacts" requirement to subject it to the jurisdiction of the U.S. federal court in California.*
[118] *See http://www.ifpi.org/site-content/library/newsletter13.pdf, p. 14. For the most recent developments, see the International Supplement to the White Paper, available at http://cyber.law.harvard.edu/media/wpsupplement2005.*
[119] *259 F.Supp.2d 1029 (C.D. Cal. 2003), aff'd, 380 F.3d 1154 (9th Cir. 2004).*
[120] *See http://news.zdnet.co.uk/business/0,39020645,39164142,00.htm.*
[121] *Id.*
[122] *See http://www.time.com/time/world/article/0,8599,203691,00.html.*

created a program that disabled the copy protection for Adobe's eBook reader. He was arrested in the United States while attending a conference where he had been invited to give a presentation on the software. The U.S. government argued that Sklyarov's copy protection circumvention violated the DMCA. Charges against Sklyarov were eventually dropped; ElcomSoft was tried and acquitted in the United States.[123]

As further discussed in the International Supplement to this White Paper,[124] the U.S. and international copyright regimes are changing in response to technological advances but despite these adjustments, the global nature of the Internet continues to pose a challenge for copyright enforcement across international borders.

[123] *An archive of documents relating to the ElcomSoft case is available at http://www.eff.org/IP/DMCA/US_v_Elcomsoft/.*
[124] *See http://cyber.law.harvard.edu/media/wpsupplement2005.*

4. Proposed and Pending Law in the United States

This section provides an overview of pending legislative proposals in the United States, which could, if passed, profoundly alter the balance of interests among copyright holders, technology providers and consumers. Before that, however, we briefly discuss a recent regulatory development concerning the technological protection of digital broadcast signals.

Regulatory development

Starting in 2006,[125] television stations will be required by statute to broadcast digital rather than analog signals. In an effort to assure the broadcast industry that rampant piracy of these digital signals will not take place, the Federal Communications Commission (FCC) enacted the **"Broadcast Flag"** regulation, effective 1 July 2005.[126] The Broadcast Flag data signal must be embedded in a broadcast to tell digital receiving equipment not to authorize certain uses of the signal, such as making second-generation copies.[127] Sale or importation of high-definition television (HDTV) receiver hardware that does not comply with the broadcaster-specified restrictions on subsequent use will become unlawful after 1 July 2005. Critics such as the EFF point out that the flag will curtail traditional fair uses such as making backup copies or playing copies on legacy devices. They also note there will be conflicts with open source software, which by definition is not resistant to user modification as the regulation requires.[128]

A similar discussion has recently emerged around **digital radio**, which transforms over-the-air broadcast into digital signals and increases the quality of audio FM signals to that of a CD.[129] Due to concerns that consumers could stop buying songs or albums from online stores and would, instead, start recording songs from digital broadcast services, the RIAA is lobbying for encrypted music transmission to make sure that only authorized receivers could play the songs according to restrictive content protection rules. In the context of a recent FCC proceeding on digital audio broadcasting, the FCC raised the question whether the government should mandate the use of **content protection** technology for digital radio.

---

[125] *Some commentators believe the transition will take longer. See http://abcnews.go.com/sections/scitech/ZDM/FCC_powell_CES_pcmag040113.html.*
[126] *See In re Digital Broadcast Content Protection, 18 F.C.C.R. 23,550 (Nov. 4, 2003) (forbidding sale or importation, after July 1, 2005, of digital television receivers or converters that do not comply with broadcaster-imposed restrictions on duplication or redistribution of content) (to be codified at 47 C.F.R. §§ 73.9000–73.9009); http://www.eff.org/IP/Video/HDTV/20031104_eff_pr.php.*
[127] *See http://www.cdt.org/copyright/broadcastflag.pdf.*
[128] *See http://bpdg.blogs.eff.org/archives/000121.html.*
[129] *See http://www.fcc.gov/cgb/consumerfacts/digitalradio.html.*

The Broadcast Flag exemplifies so-called "technology mandates." In 2002, Senator Fritz Hollings introduced the Consumer Broadband and Digital Television Promotion Act (CBDTPA), a bill that would have mandated copyright protection technologies in all digital media devices. The bill was wider in scope than the Broadcast Flag and could have extended to cell phones, computers, digital hearing aids[130] and even refrigerators[131]—barring many fair use applications of existing consumer electronics products (see below). The CBDTPA did not become law (having failed to emerge from the Senate Committee on Commerce, Science and Transportation), but may nevertheless serve as an exemplar for future regulatory efforts.

Proposed legislation

Family Entertainment and Copyright Act of 2004[132]
Introduced: 20 November 2004
Status: Passed Senate 20 November 2004; received in House, 24 November 2004

The Family Entertainment and Copyright Act amalgamates provisions from a number of intellectual property-related bills, including the Artists' Rights and Theft Prevention Act (S. 1932), which prohibits using an audiovisual recording device to make copies of movies in theaters; the Family Movie Act (HR 4586), which creates an exemption from copyright infringement for editing or obscuring parts of motion pictures for private home viewing (to protect ClearPlay[133]); the National Film Preservation Act (HR 3569), which funds a Library of Congress effort to preserve rare films; and the Preservation of Orphan Works Act (HR 5136), which lets libraries make copies of works in the last 20 years of their term that are not commercially exploited nor available at a reasonable price; the Anticounterfeiting Act of 2004 (S. 2227), which prohibits counterfeiting labels, documentation, packaging or authentication on phonorecords, computer programs and audiovisual works; the Fraudulent Online Identity Sanctions Act (HR 3754), which penalizes false provision of domain name registration information or falsely registers a domain name; and the Cooperative Research and Technology Enhancement Act (CREATE) (HR 2391), which overrules a Federal Circuit decision limiting patentability of inventions from collaborative efforts. In the last minute, the Senate dropped a section (HR 4077, see below) which would have introduced new criminal penalties for file-sharers and would have lowered the standard for copyright infringement.[134]

Inducing Infringement of Copyrights Act of 2004[135] (IICA or INDUCE Act) (S. 2560)
Introduced: 22 June 2004
Status: Referred to the Senate Committee on the Judiciary. Congressional term ended without passage

[130] *See http://www.widexusa.com/senso_diva.html.*
[131] *See http://www.amana.com/sidebyside/messengersimulation.html.*
[132] *See http://thomas.loc.gov/cgi-bin/query/z?c108:S.3021:.*
[133] *See http://www.clearplay.com/FamilyMovieAct.aspx.*
[134] *See http://www.wired.com/news/politics/0,1283,65796,00.html.*
[135] *See http://thomas.loc.gov/cgi-bin/bdquery/z?d108:s.2560:.*

The INDUCE Act, sponsored by a bipartisan coalition of senators, would enable civil lawsuits by copyright holders against any party that "induces" illegal copying by another. The Act responds[136] to the District Court's decision in *Grokster*, which stated that a secondary liability theory against P2P services might be warranted, but "additional legislative guidance may be well-counseled."[137] Opponents criticized the bill's text[138] for being overbroad, for potentially creating liability for unforeseen parties such as technology makers[139] and for potentially overturning the landmark *Sony v. Universal* decision (the *Betamax* case). The Ninth Circuit's recent affirmation of the *Grokster* decision[140] (discussed above) has increased support for the INDUCE Act.

Piracy Deterrence and Education Act of 2004[141] (HR 4077)
Introduced: 31 March 2004
Status: Passed by House, received in Senate, 29 September 2004

The Piracy Deterrence and Education Act of 2004 would authorize the Attorney General to develop a program under which the Department of Justice could send—via ISPs—warning letters to alleged copyright infringers. Further, it would direct the Attorney General to ensure that any unit in the Department of Justice responsible for investigating computer hacking or intellectual property crimes is assigned at least one support agent who has received training in the investigation and enforcement of such crimes. Moreover, it would require that an Internet Use Education Program be established within the Office of the Associate Attorney General, a program aimed at educating the public about the value of copyrighted works and the effects of their theft.

It integrates provisions from the Artists' Rights and Theft Prevention Act of 2004, or ART Act, making the unauthorized use of a video camera in a movie theater in order to transmit or make a copy of a copyrighted a criminal offense (fine or imprisonment up to three years). Further, the Piracy Deterrence and Education Act would amend federal copyright law to provide criminal penalties, as well as civil remedies in damages, for the willful infringement of copyrighted works as well as the "offering for distribution" to the public by electronic means "with reckless disregard of the risk of further infringement."

Protecting Intellectual Rights Against Theft and Expropriation Act of 2004[142] (PIRATE Act) (S. 2237)
Introduced: 25 March 2004
Status: Passed by Senate; Referred to House Subcommittee on Courts, the Internet, and Intellectual Property, 4 August 2004

---

[136] *The Washington Post, referring to Grokster, quoted sponsor Sen. Orrin Hatch as saying, "[T]he legislation is partly in response to the California decision." See http://www.washingtonpost.com/wp-dyn/articles/A801-2004Jun23.html; see also http://news.com.com/Senator+wants+to+ban+P2P+networks/2100-1027_3-5280384.html.*
[137] *259 F.Supp.2d 1029, 1046 (C.D. Cal. 2003).*
[138] *See http://www.lessig.org/blog/archives/COE04694_LC.pdf.*
[139] *The EFF drafted a mock legal complaint against Apple, Toshiba, and CNET relying on the pending legislation. See http://www.eff.org/IP/Apple_Complaint.php.*
[140] *See Metro-Goldwyn-Mayer Studios et al. v. Grokster et al. (9th Cir. 2004), at http://www.ca9.uscourts.gov/ca9/newopinions.nsf/E9CE41F2E90CC8D788256EF400822372/$file/0355894.pdf?openelemen.*
[141] *See http://thomas.loc.gov/cgi-bin/query/z?c108:H.R.4077:.*
[142] *See http://thomas.loc.gov/cgi-bin/bdquery/z?d108:s.2237:.*

Senator Patrick Leahy's PIRATE Act of 2004 would empower the Justice Department to file civil suits against P2P users suspected of copyright violations. While the RIAA has already filed thousands of lawsuits against individual file-sharers, proponents of the PIRATE Act argue that more legal power is needed. According to bill co-sponsor Senator Orrin Hatch, optimal deterrence of file-sharers, potentially via "tens of thousands" of lawsuits, requires bringing to bear the resources and "moral authority" of government.[143] Leahy cites the difficulty of meeting the high-proof threshold for criminal charges to argue that prosecutors should be able to pursue civil charges.

Critics counter that industry lawsuits against file-sharers are already a suboptimal mechanism for resolving online copyright infringement conflict and that the industry does not need the Justice Department's help pursuing them. Additionally, opponents note that U.S. taxpayers would bear the expense of lawsuits designed to protect the profits of media companies, many of which are based overseas. Some legal commentators cite the bill's troubling implications for the "double jeopardy" doctrine, since the bill would expose file-sharers to two lawsuits—one by the government and one by the copyright holder. Finally, the speed at which the bill has moved through the legislative process, passing the Senate unanimously, has raised concerns about whether appropriate deliberation has been undertaken.

Digital Media Consumer's Rights Act[144] (DMCRA) (HR 107)
Introduced: 7 January 2003
Status: House Subcommittee on Courts, the Internet, and Intellectual Property (hearings held), 12 May 2004

The DMCRA seeks to restore fair use rights under the DMCA by declaring that circumvention of a technological measure must result in copyright infringement for the circumvention to create liability.[145] The measure also protects the distribution and use of tools that circumvent technological restrictions if those tools enable significant non-infringing use of a copyrighted work. Finally, the DMCRA explicitly protects circumvention when necessary for scientific research and mandates labels on copy-protected CDs. Some critics believe the last provision will unnecessarily increase CD production costs, thus hurting consumers. Consumer rights advocates widely support the bill, lauding it as a reaffirmation of the fair use doctrine.

Benefit Authors without Limiting Advancement or Net Consumer Expectations Act of 2003 (BALANCE Act) (HR 1066)
Introduced: 4 March 2003
Status: Referred to House Subcommittee on Courts, the Internet, and Intellectual Property, 5 May 2003

---

[143] *See http://news.com.com/2100-1027_3-5248333.html.*
[144] *See http://www.house.gov/boucher/docs/BOUCHE_025.pdf.*
[145] *The DMCRA, proposed by Rep. Rick Boucher, is identical to the bill Boucher introduced at the end of the Congressional session in 2002.*

The BALANCE Act modifies the Copyright Act and the DMCA to better protect consumers.[146] First, it would allow consumers to circumvent technological restrictions to make fair use of digital media. Second, it would re-establish the first sale doctrine, allowing consumers to resell digital media. Third, it would prohibit non-negotiable licenses that restrict fair use rights.

Anti-Counterfeiting Amendments of 2003[147] (HR 3632)
Introduced: 21 November 2003
Status: Passed by the Senate on 20 November 2004, as part of the Family Entertainment and Copyright Act of 2004

The proposed Amendments would criminalize trafficking in items that alter or mimic "authentication" systems like watermarks, holograms or serial numbers.

Peer-to-Peer Piracy Prevention Act[148] (HR 5211)
Introduced: 25 July 2002
Status: Referred to House subcommittee

Rep. Howard Berman's bill would release copyright holders from liability when they take technological steps to stop copyright infringement on a P2P system. Supporters—mostly from the entertainment industry—claim that allowing copyright holders "self-help" against infringement is no different than allowing homeowners to protect themselves against burglars.[149] They argue that the bill is sufficiently limited to ensure that copyright holders will be permitted to do no more than necessary to protect themselves and that P2P users who have been unfairly harmed will have legal recourse. Critics argue that attacks on alleged infringers may harm individual computers, P2P systems or even the Web as a whole. Some warn of a potential "technical arms race" as P2P services alter their programs to defend against these attacks.

Music Online Competition Act[150] (HR 2724)
Introduced: 21 August 2001
Status: Referred to the Subcommittee on Financial Institutions and Consumer Credit

Drafted by Rep. Rick Boucher, the Music Online Competition Act would mandate nondiscriminatory licenses to online music vendors and would ease the royalty collection process for vendors and artists. The bill was created in lieu of antitrust investigations into MusicNet and Pressplay, two of the music industry's online distributors.

International treaties

World Intellectual Property Organization (WIPO) Broadcast Treaty[151]

---

[146] *Representative Zoe Lofgren's BALANCE Act of 2003 is a slightly updated version of the Digital Choice and Freedom Act of 2002, introduced near the end of the last Congress in 2002.*
[147] *See http://thomas.loc.gov/cgi-bin/bdquery/z?d108:h.r.03632:.*
[148] *See http://thomas.loc.gov/cgi-bin/bdquery/z?d107:h.r.05211:.*
[149] *Example from http://www.heritage.org/Research/InternetandTechnology/EM835.cfm.*
[150] *See http://www.house.gov/boucher/moca-page.htm.*
[151] *See http://www.wipo.int/documents/en/meetings/2004/sccr/pdf/sccr_11_3.pdf.*

Consolidated Text Dated: 29 February 2004
Status: Awaiting recommendation for diplomatic conference

The WIPO Broadcast Treaty, or the Treaty on the Protection of Broadcasting Organizations, would bestow upon broadcasting organizations[152] potentially unprecedented levels of control over the content they broadcast. Article 8, Right of Fixation, simply states: “Broadcasting organizations shall enjoy the exclusive right of authorizing the fixation of their broadcasts.” Fixation refers to copying or recording. Article 9 grants broadcasters the right to control whether copies of copies can be made. Finally, Article 15 requires signatories to make the protections last for 50 years, while Articles 16 and 17 contain DMCA-like anti-circumvention provisions to help broadcasters enforce the treaty’s new rights.

Critics of these provisions—including non-governmental organizations[153]—point out the provision would protect content currently in the public domain that enjoys protection under copyright law. They further argue that this severe constriction on the public domain lacks justification and that providing 50 years of protection every time something is broadcast is tantamount to an endless copyright. A diplomatic conference to adopt the treaty is pending.

[152] *Including Webcasters in the treaty is currently under debate.*
[153] *See, e.g., http://www.eff.org/deeplinks/archives/001599.php; see also http://www.public-domain.org/node/view/38?PHPSESSID=24d214d72b7e2b75b4c4e8c80bcaec57.*

5. Digital Rights Management

DRM refers to the use of technology to manage how copyright holders' intellectual property such as songs, movies, pictures and texts can be used. DRM systems include technological restrictions on playing, copying and distributing content. This section provides a brief introduction to DRM, discusses what current *de facto* standards are, points to challenges and unresolved issues, and outlines a workable DRM solution.

Special emphasis lies in this section on the DRM protection of online music distribution, the first significant market that has been heavily using DRM schemes. The Digital Media Project will continue to research DRM applications in the markets for digital distribution of movies,[154] TV content and printed materials, which have distinct characteristics and face different challenges.

DRM essentials

Content protection technology, such as DRM software, enables a content provider to "wrap" a set of rules around content that defines if and how the purchaser of the copyrighted or premium content can manipulate and share it. The rules can include, for instance, how many copies of the original file a user may make, whether a back-up or archive file can be created, and whether a user can move the content to another device. Typically, content is encrypted; to get the decryption key, a user must act—for example, by paying money, providing an e-mail address or agreeing to permit tracking. DRM software vendors deliver the tools, but content owners set the conditions.

At the heart of all DRM technology is a rights model. Rights models are schemes for specifying rights to content that a user can obtain in return for some consideration. DRM software can define rights to content according to a rights model, and then enforce those rights. To function effectively, DRM software must understand the core entities and the relationships between them.[155]

Rights models follow multiple schemas. These include the Open Digital Rights Language. In Open Digital Rights Language, if a right is not explicitly permitted, it is prohibited. For example, an Open Digital Rights Language agreement may state a particular video can be played a maximum of 10 times (a count constraint) in any semester (that is, a temporal constraint) for a $10 fee (a requirement to pay).

---

[154] *See, e.g., Derek Slater, Meg Smith, Derek Bambauer, et al., Content and Control: Assessing the Impact of Policy Choices on Potential Online Business Models in the Music and Film Industries, available at http://cyber.law.harvard.edu/media/content_and_control.*

[155] *See Anthony Allen, Digital Rights Management Software: Perspective (Gartner, Inc.), October 3, 2002. Report # DPRO-93479.*

DRM technologies often employ measures such as watermarking, signatures, nonrepudiation and secure delivery. Digital watermarking embeds invisible markings into a digital object to track how its content is used and accessed. Digital signatures use public/private key cryptography to provide user authentication that verifies the user's identity. Nonrepudiation uses digital signatures to prove that a particular sender sent a message (e.g., an online subscription service might want to prove it delivered requested content) and that a recipient received a message (e.g., the customer of the online subscription service). Secure content delivery guarantees electronic delivery using secure document hosting and e-mail notification (e.g., to notify a recipient of a pending document and to notify the sender that the document was retrieved).

De facto standards

Controlling media distribution and consumption requires industry standards that deliver the interoperability needed for consumers and media companies to select and deliver content across multiple networks, services and devices. One language gaining ground is the extensible rights markup language (XrML). XrML is designed to be a universal way to specify and securely manage rights and other conditions for all kinds of resources, including digital content and services. Supporters argue that the technology can help deliver the interoperability required to build "end-to-end" DRM solutions.

Some of the current de facto standards are:

- **Content scrambling system.** CSS, developed by various industry groups, is the encryption standard used to "lock" all commercial DVDs containing copyrighted material. The content is compressed and encrypted on a disc with one set of "keys" embedded in the code. The other keys are located in DVD players. The disc looks for the keys on the machine and, once matched, plays the disc. Jon Johansen's DeCSS program is shareware, making it one of many decryption tools available on the Internet allowing users to unlock the code on a DVD, open it and copy its content.

- **Adobe Systems PDF technology.** Adobe's Acrobat is used to read print content protected by Adobe's Acrobat authoring tools (PDF files). The reading software can be downloaded and used for free, but the authoring tools must be purchased. As noted in the *ElcomSoft* case, the "locks" on PDF files have been picked.

- **Music and video.** By the end of 2004, a number of legitimate online music stores in the United States, Canada and the European Union ship content

"wrapped" or protected by DRM technologies.[156] Among the better-known services and DRM technologies are:

- **Apple's iTunes music store.** AAC-based music files are wrapped with Apple's proprietary FairPlay DRM technology.

- **Napster's online music store.** Sells content in Microsoft's WMA wrapped with Microsoft's Windows DRM. In January 2005, Napster stated it would enable costumers of its premium subscription service to have subscription "portability" (i.e., the ability to move subscription content onto portable devices), functionality not previously available for customers of its premium service, if they pay an additional $5 fee (bringing the total to $14.95/month). The enabling technology for this instance of subscription portability is Microsoft's "Janus" DRM, included in WindowsDRM 10. (See next section for additional information.)

- **Virgin Digital.** This is Virgin's online music store selling à la carte downloads. Content is shipped in WMA format and protected by WindowsDRM.

- **MusicMatch.** Uses Microsoft's WMA and DRM technologies. (Yahoo purchased MusicMatch at the end of 2004 and has not yet articulated how the MusicMatch technology and assets would be utilized.)

- **Sony's Connect online music store.** Delivers content in its proprietary ATRAC format wrapped with the company's WDM DRM.

- **Real's Online Music Store.** Offers content encoded in AAC and wrapped in Real's proprietary HelixDRM.[157]

- **WalMart's online store.** Selling à la carte downloads. Content is delivered in the WMA file format and protected with WindowsDRM.

In the previous sections, the discussion focused on protecting digital music files (with the exception of the discussion regarding movies on DVDs). However, the use of DRM to protect commercial music CDs has been discussed for the past two or three years. By late 2003 and into 2004, record companies and technology companies discussed publicly and then shipped limited numbers of **copy-protected CDs.** Copy-protected CDs

---

[156] Is it possible to evade FairPlay, WindowsDRM, or HelixDRM? Yes. A user can burn songs in WMA or AAC onto a CD. The user can then remove those songs' DRM protection simply by re-ripping this CD back on a hard drive in the MP3 format. This causes the degradation in sound quality that occurs when any audio file is compressed, decompressed, or recompressed, but allows users to bypass DRM.

[157] Real offers technology allowing consumers to play its songs on Apple's iPod portable music players. Apple opposes the move and threatens to change the iPod software to end Real's compatibility. See Laurie J. Flynn, Apple Attacks RealNetworks Plan to Sell Songs for iPod, N.Y. Times, July 29, 2004, at C3.

have already led to a controversy on the European market and before European Courts.[158] New technologies enable greater control over physical media. For example, Microsoft's Windows Media Data Session Toolkit provides tools for developers to create solutions for copyright holders and content providers such as record labels. It lets content producers ship "dual-session" or "second-session" CDs. The first session contains the work in a secure format. The second session is protected with Windows Media DRM. The second session version can have multiple rules or rights that enable a consumer to take some actions, such as moving content to a portable device, but also limit the number of times certain tracks can be burned to a CD. Initial commercial dual-session CDs were unreliable—they frequently did not play in standard commercial CD players, let alone PCs with CD drives. Other technologies, such as those from SunComm, Macrovision and First4Internet, have matured to the point where a dual-session CD by Velvet Revolver went to the top of the U.S. charts in April 2004 with no apparent consumer backlash. Ironically, some P2P file-sharing tools are boosting interest in use of DRM technologies. For example, online music provider AltNet uses DRM to allow customer-to-customer music sharing via transfers of DRM-restricted files (similar to the Weed product mentioned previously).[159] The DRM imposes limits such as allowing only three plays of a song before the user must purchase the track.

Conflicting standards

Recently, conflicts between technology companies and content providers about compatibility and interoperability of DRM standards have emerged. Apple established early leadership in the online music market with its iTunes Music Store and iPod player. As a result, other online music services sought to sell AAC-FairPlay content to iPod users. Apple's leadership rebuffed these entreaties. In response, Real Networks released Harmony Technology in July 2004 (see also above). This software program allows consumers to buy content from Real's online store—packaged in Real's AAC/HelixDRM-based formats—convert it to Apple's AAC/FairPlay format, and play it on their iPods.[160] Real claims it did not violate the DMCA's anti-circumvention provisions and that it created the technology because Apple refused to license its technology. Real announced a special 49-cents-per-song promotional effort to get consumers, especially iPod users, to come to the Real online store. Apple said little publicly, stating only that company lawyers and engineers were reviewing the Harmony code and expressing surprise that Real adopted the methods and ethics of a "hacker" in creating Harmony.

---

[158] See International Supplement to this White Paper, available at http://cyber.law.harvard.edu/media/wpsupplement2005.
[159] See http://www.abc.net.au/news/newsitems/200407/s1149743.htm; see also http://www.altnet.com/products/reduce.asp; http://news.findlaw.com/ap/ht/1700/7-28-2004/20040728053004_22.html.
[160] See http://news.com.com/RealNetworks+breaks+Apple%27s+hold+on+iPod/2100-1027_3-5282063.html.

An already volatile arms race of marketing and technology is likely to intensify after Microsoft opened its online music store in October 2004. MSN Music is an à la carte download store. Late in 2004, Microsoft debuted a form of DRM, code-named "Janus." Janus enables subscription music service providers such as Napster and MusicMatch to let consumers download content and move it to portable devices—a benefit subscription services have not been able to offer. Janus-enabled content and devices essentially link up every time the portable device is hooked to the host PC and synchronized. There's a secure time clock in both the PC and portable device system. If the user quits the subscription service or does not their pay bills after a predefined period of time—say the expiration of the previous 30-day cycle for which the consumer paid—all the content is effectively erased from the PC and the portable device. If Janus works as promised, it could deliver to consumers the "celestial jukebox" in which all commercial music would be available to them at any time on virtually any device—as long as the device and service can authenticate the user and their subscription status.

The Apple-Real contest underscores that while DRM compatibility and interoperability remain long-term market inhibitors, the actual market—consumers—has not yet been heard on this topic. This will change as more consumers move to online channels to obtain content and look to use that content in greater numbers of disparate devices.

Challenges and policy issues

DRM schemes have become critical elements of digital content distribution in general and online music distribution models in particular. However, DRM is not a simple answer to the problem of increased vulnerability of digital content distributed over electronic networks. Rather, DRM is itself a complex and evolving concept, which faces challenges not only from a technological perspective, but also from a business and legal/regulatory perspective. The increased use of DRM technologies aimed at limiting users' behavior—and often also limiting traditional rights and privileges such as fair use and first sale (see above)—is an area of growing public concern. **Policy considerations**, among other things, include the following important issues:

- **Usage rights.** Through DRM, the delicate balance between the interests of copyright holders and the public can be upset or may even be completely overridden. Because anti-circumvention legislation here and abroad[161] does not (or only to a limited extent) provide exceptions for fair use or fair dealing and first sale, copyright holders and intermediaries can (and often do) use DRM to unilaterally determine users' freedoms.[162] From a policy perspective, such restrictions are troublesome because DRM can thus limit various personal and transformative uses and, ultimately, undermine the promise of the digitally networked

[161] *See the International Supplement to this White Paper, http://cyber.law.harvard.edu/media/wpsupplement2005.*
[162] *Contract law can aim towards similar results, but, unlike DRM, its impact is not self-enforcing. For further discussion of these issues, see, e.g., Urs Gasser, John Palfrey, Derek Slater et al., iTunes: How Copyright, Contract, and Technology Shape the Business of Digital Media—A Case Study, June 2004, available at http://cyber.law.harvard.edu/media/itunes.*

environment, which enables the transformation of passive consumers into active users with the ability to interact with and manipulate content.

- **Innovation and competition.** DRM schemes might be used by copyright holders and DRM standard creators to "lock out" disfavored digital media devices and software creators. Often, the use of a proprietary DRM standard allows vendors such as Apple to control secondary markets. Currently, for instance, only iTunes and Quicktime software can play FairPlay files, and the iPod is the only compatible portable player. Further, the DMCA bolsters control by restraining reverse engineering. Without the DMCA, skilled programmers could analyze how the DRM works to create, for example, compatible players without fear of liability. This interplay between technology and law allows for the deployment of a market strategy based on excluding competition through restricted interoperability[163]—a strategy that might be sound from a business perspective. From the policy perspective, however, this approach prevents innovation and, ultimately, may not render the optimal welfare-enhancing result.

- **Privacy.** In the process of their operation (consider, for instance, the purchase of a music file via an online music store), DRM systems often collect and further process information that relates to an individual and enables the identification of this person. These DRM-based data processing practices raise red flags from a privacy perspective. Areas of particular concern include the use of DRM schemes for collecting purposes without a user's consent or knowledge, detrimental effects on personal integrity and dignity (e.g., interference with the "right to read anonymously"[164]), and the re-use of personal data for secondary purposes (e.g., litigation and marketing). However, DRM supporters argue that technology can also be used to safeguard privacy ("privacy enhancing technology"). Against this backdrop, scholars and researchers have suggested models aimed at merging DRM schemes with privacy rights management systems.

Even more fundamentally, however, the functional legitimization of DRM systems as such is disputed.[165] Many believe that DRM is an ineffective barrier to **piracy.** DRM critics argue—and security experts agree—that no DRM is uncrackable. Consequently, DRM cannot prevent that unencrypted copies (in fact, one copy suffices) can quickly propagate through P2P networks. If DRM cannot prevent piracy and does not affect the viability of P2P, so the argument goes, it may only diminish the value of the purchased

[163] *See John Palfrey, Holding Out for an Interoperable DRM Standard, in Christoph Beat Graber, Carlo Govoni, Michael Girsberger, and Mira Nenova (eds.), Digital Rights Management: The End of Collecting Societies? (Forthcoming, April 2005.)*
[164] *Julie E. Cohen, A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace, 28 Conn. L. Rev. 981 (1996), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=17990.*
[165] *For further discussion, see Urs Gasser, John Palfrey, Derek Slater et al., iTunes: How Copyright, Contract, and Technology Shape the Business of Digital Media—A Case Study, June 2004, available at http://cyber.law.harvard.edu/media/itunes.*

content and, ultimately, decrease consumer demand. DRM supporters, by contrast, argue that a certain degree of leakage is acceptable, and that DRM, in combination with litigation and educational campaigns, can significantly reduce piracy.

While the potential future effects of widely applied DRM systems on piracy remain unknown, the mere **uncertainty** about its effectiveness in combination with the well-established areas of concerns call for a **cautious approach**, especially regarding potential legal interventions aimed at backing-up DRM schemes (e.g., in the form of restrictive anti-circumvention legislation), or with regard to legislative as well as regulatory attempts to mandate technological protection measures in media devices.

A possible model

The previous paragraphs have made clear that DRM technologies are important but that the way in which they are applied is even more critical. From a business perspective, DRM will be deployed and refined as long as content control and copy protection remain top priorities for digital media publishers. To avoid alienating consumers, DRM standards must be flexible enough to protect content, to be replaced when hacked, and to accommodate changes in consumer behaviors and the tenets of fair use—all of which can be disrupted by new technologies. Achieving this balance is problematic given the fact that technology or "code," as Professor Lawrence Lessig of Stanford University Law School states, can never accurately map evolving legal doctrines such as fair use.

A workable, sustainable and balanced DRM solution would minimize the inevitable tensions, tradeoffs and dilemmas as much as possible. One possibility is for media companies to adopt an approach to content distribution that GartnerG2 calls **"perfectly portable content."** Perfectly portable content seeks to balance the needs for access and control of digital content distributed on the Web. Perfectly portable content allows copyrighted content to move from device to device under a user's control. At any point in time, a piece of content exists in only one instance (though more than one instance is possible, depending on the rules established by the copyright holder or publisher), which can be viewed on a PC, PDA or any other device that can be authenticated. Content can be "locked" by authenticating the digital certificates used by DRM technologies. Perfectly portable content meets publishers' needs to prevent unauthorized and uncompensated copies while giving consumers a sense of ownership and the ability to engage in fair use manipulation of their legitimate digital content.

In practice, the perfectly portable content model might work like this:

- A copyright holder/media company releases a new copyrighted work—in this case, a Patricia Barber CD. The company requires the manufacturer to include in the copy a basic set of rules for how the content can be used (for example, using an XrML-based set of tools). The core of the perfectly portable content concept is that, at any one time, there are a preset number of active

instances of the content. Users can make a specific number of copies of a song or the entire CD, and a preset number of tracks—or the entire CD—can be ripped into MP3 files and moved onto a portable MP3 player.

- A consumer who purchased the Patricia Barber CD (or a set of files representing each track of the music CD) decides to loan it to someone else who listens to it.
- While the CD owner's friend has the CD either in physical or digital format, the owner cannot listen to it unless the content's rules allow her to burn a second CD for time- or location-shifting.
- The borrower, who likes Patricia Barber after listening, buys a copy of the CD and returns the original to the owner. Or in a digital distribution model, the borrower samples the tracks that comprise the CD, and returns the files or the CD to the original owner.

Theoretically, it is easy to ascribe specific rules of ownership to digital content and inject them into the media itself. These same rules can be transferred, protecting the first sale concept. Early market experience indicates few consumers have encountered problems with Apple's iTunes content, Napster's WMA- and WindowsDRM-protected content, or Real's HelixDRM-protected content. However, this lack of controversy likely results from the relatively immature state of the online music (and media) market. For example, GartnerG2 conservatively forecasts that U.S. households will spend approximately $1 billion in online music by 2008. However, this still only represents a fraction of the prerecorded music market in the United States, which measured $13 billion in 2003.

Perfectly portable content may help maintain a healthy balance in the relationship between consumer electronic device manufacturers and content providers, preventing one from exerting a disproportionate influence over the other. Content providers depend on device manufacturers delivering products compatible with their content and delivering the best playback performance of that content for end users. Technology providers must ensure compatibility with the most popular content. As discussed above, conflicts between the parties can arise from such technology, as with the controversy surrounding artists' rights to be paid for tracks on a dual-session disc's second session.[166]

[166] *See http://news.com.com/Rights+issue+dogs+CD+protection/2100-1027_3-5139762.html?tag=st.rn.*

6. What's Ahead

Digital technologies and digital media content—from entertainment to reference material—have become more portable in time, space and format. Content providers, though, have been slow to adapt to digital distribution for fear of crushing old business models before they devise new ones. Industry players generally implement digital technology to protect existing business and aggressively pursue perceived abusers of copyrighted material. They have solicited and received assistance in these efforts from legislators in the form of the DMCA and other legislation aimed at preventing what they perceive as illegal copying or sharing.

Digital advancements have exacerbated the historic tension between copyright holders (generally the entertainment industry), technology providers and consumers, especially for recorded music, movies and print.

The law

Laws protecting content providers and copyright holders have become increasingly restrictive. Two examples are the DMCA's "anti-circumvention tools" provisions and Congress' continued extensions of copyright terms. The extraordinary control exerted by copyright holders/content providers extends along the digital media value chain, from creation and production to distribution and, with DRM tools, to playback. The Constitution's original objective in protecting intellectual property was to encourage innovation by providing creators exclusive rights for limited times. This objective has been subverted to the extent that new legislation and copyright term extensions stifle legitimate and desirable innovation, improvement or creation based on works in the public domain.

An analysis of current digital media distribution schemes suggests that copyright holders and content companies are using two interacting concepts beside copyright law to control user's behavior: contract law and legal provisions aimed at backing up technological protection measures.[167]

- Contract law—in the digital media context appearing in the form of "terms of service" or "license agreements"—limits what consumers can do with purchased digital content such as online music, movies or e-books. License agreements often override rights consumers would otherwise enjoy under copyright law. Thus, for instance, license agreements of online music services often prohibit users from reselling, lending or transferring songs—rights usually granted by the first sale doctrine or fair use in the United States. As discussed above, current case law and precedents hold that courts will generally

[167] *See, e.g., Urs Gasser, John Palfrey, Derek Slater et al., iTunes: How Copyright, Contract, and Technology Shape the Business of Digital Media—A Case Study, June 2004, available at http://cyber.law.harvard.edu/media/itunes.*

enforce such contracts over an entitlement authorized by Congress under the Copyright Act.

- As demonstrated in this White Paper, digital content providers are increasingly turning to technological protection measures to constrain usage of e-content. To take a prominent example, the iTunes Music Store restricts transformative use of music and limits the number of burns with the exact playlist via FairPlay. Technological protection measures are increasingly supported with strong laws prohibiting the circumvention of DRM that protects copyright holders' exclusive rights (see above). As discussed in the International Supplement to the White Paper,[168] this trend is global in nature. Accordingly, copyright holders here and abroad can, by and large, rely both on self-enforcing technical protection measures and strong anti-circumvention provisions.

Growing limitations on users' access to and use of digital content are troublesome from a policy perspective, since they significantly shift the delicate balance between copyright holders' interests on the one hand and the public's interests on the other.

The legislation

The legislative outlook at the federal level is decidedly mixed. Several pending pro-consumer and technology industry bills would expressly protect fair use for consumers using digital media, manufacturers of products that permit such fair uses, and scientific research efforts on technology protection measures.

Ready to counter those measures are bills sponsored by the entertainment industry, including measures that would require manufacturers of products to incorporate technological measures into digital products to prevent copying, whether fair or unfair, and provide private causes of action and stiff penalties for civil and criminal violations. It is hard to predict which, if any, of the bills will be enacted into law. No action will likely be taken on many of these copyright matters until various international conflicts and economic matters are resolved. Recently, however, it has been observed that the INDUCE Act gained support in Congress as a consequence of the affirmative *Grokster* ruling by the Ninth Circuit Court (see above).

The business

The music industry is the first to face the potential benefits and terrors of digital distribution. The digital channel offers the ability to deal directly with buyers without the expense of a physical distribution network, but creates the uncertainty of competing with "free" content.

[168] *See http://cyber.law.harvard.edu/media/wpsupplement2005.*

- **Challenge:** Securing digital transactions and, in light of KaZaA, eDonkey, BitTorrent and other P2P networks, creating a compelling alternative to decentralized file-sharing networks remains the key challenge. SNOCAP technology, as mentioned previously, seeks to create a method for legitimizing much of the traffic on P2P networks.

- **Benefits:** The Internet and new technologies have proven extremely effective marketing tools for the music companies and musicians. As innovators continue to innovate, services aimed at creating legal-sharing opportunities, such as Grouper and Mercora, can expand the promotional and advertising opportunities for musicians and labels. These efforts augment the fact that labels and musicians are already using Web sites to promote new releases while providing samples and near-instantaneous access to an artist's catalog of content. These benefits promise to help open up the commercial potential of the "back catalogs" each of the labels owns, content that has not been available in years due to limited demand. Labels can use Web sites to promote new releases and provide samples and near-instantaneous access to an artist's catalog of content—including content not available through physical media due to limited demand.

In visual entertainment content, particularly TV broadcast programming, new technologies threaten to destroy the ad-heavy business models of U.S. television broadcasters. PVR technology threatens existing TV network revenues, as well as back-catalog movies and other potential packages of older TV and film content, while at the same time offering new opportunities.

- **Challenge:** Time-shifting TV programming will eventually make the notion of "prime time" and advertising rates obsolete.

- **Opportunity:** Advertising-dependent TV broadcasters must explore new advertising models, including sponsorship, product placement and targeted advertising, to sustain the revenues needed to produce new content.

Stop the rhetoric and start framing the future

In an attempt to stop the rhetoric and start talking about practical solutions, we have identified **five scenarios** as possible outcomes of technological, business, legislative and legal developments:

- The **No-Change Scenario**[169] assumes that confusion remains about doctrines like fair use and first sale as the DMCA and copyright law continue to guide digital media distribution.

[169] *See http://cyber.law.harvard.edu/media/scenario1.*

- The **Speedbumps Scenario**[170] predicts that technological restrictions like encryption will create small barriers to users' access and control of digital content.

- The **Technology Lockdown Scenario**[171] projects that restrictive DRM schemes will unilaterally determine users' experience of the content they purchase.

- The **Alternative Compensation System Scenario**[172] imagines that users access digital content through a state-run system that taxes consumers according to use and rewards creators according to the popularity of their work.

- The **Entertainment Co-op Scenario**[173] envisions that voluntary associations emerge within the existing copyright structure to allow distribution of digital content between subscribers and creators.

We have analyzed—and will further discuss—these scenarios in a series of publications as potential models for distribution of digital content. All research papers and other materials are available at the Berkman Center's Digital Media Project Web site.[174] Selected reports are also available on the GartnerG2 site on the "Digital Media Transition"[175] page.

[170] *See http://cyber.law.harvard.edu/media/scenario2.*
[171] *See http://cyber.law.harvard.edu/media/scenario3.*
[172] *See http://cyber.law.harvard.edu/media/scenario4.*
[173] *See http://cyber.law.harvard.edu/media/scenario5.*
[174] *See http://cyber.law.harvard.edu/media/.*
[175] *See http://www.gartnerg2.com/spr/spr-2004-02-03.asp*

7. Contributors

For The Berkman Center

- Urs Gasser, Team Leader
- Tim Armstrong
- Derek Bambauer
- Andrew Bragin
- Blythe Holden
- Renny Hwang
- Ron Lazebnik
- Edward Locke
- John Palfrey
- Cyril Rigamonti
- Derek Slater
- Meg Smith
- Donna Wentworth

For GartnerG2

- Mike McGuire, Team Leader
- James Brancheau

Questions or comments about this document can be sent to:

- John Palfrey, Executive Director, Berkman Center for Internet & Society at Harvard Law School: jpalfrey@cyber.law.harvard.edu

- Mike McGuire, Research Director, GartnerG2: michael.mcguire@gartner.com

The team wishes to thank Mary Bridges and Erica George for their invaluable assistance.