DePaul University
University Libraries

DePaul Journal of Art, Technology & Intellectual Property Law

Volume 11
Issue 1 *Spring 2001*

Article 2

Copyright Enforcement in the Internet Age: The Law and Technology of Digital Rights Management

Stephen M. Kramarsky

COPYRIGHT ENFORCEMENT IN THE INTERNET AGE:

THE LAW AND TECHNOLOGY OF DIGITAL RIGHTS MANAGEMENT

Stephen M. Kramarsky[*]

I. INTRODUCTION: TECHNOLOGY AND THE COPYRIGHT LAW

Digital information comes in many forms; an application such as Microsoft Word, a database of consumer information collected by an e-commerce website and a feature film stored on DVD are just a few examples. Each form of digital information is protected by a different set of laws and regulations serving a different range of policies. For example, commercial software is protected by copyright, but also by the individual "shrink wrap license" under which it is distributed.[1] On the other hand, electronic databases may enjoy the protection of specialized federal or state laws or regulations that are designed to safeguard the privacy of individuals' sensitive information.[2]

---

* Stephen Kramarsky is a member of the firm of Dewey Pegno & Kramarsky LLP in New York whose practice focuses on technology and intellectual property issues in both litigation and transactional contexts. Prior to resuming private practice, Mr. Kramarsky was a founder and General Counsel of the Gryphon Group LLC, an New York Internet software and services. The author gratefully acknowledges the contributions of Nicholas R. Givotovsky in shaping his thinking about commercial digital rights management systems.

1. Most software is not actually "sold" to end users (though that fact might surprise the users themselves); it is licensed. The terms of these licenses thus typically govern the use of software (as limited by individual state contract laws). The controversial Uniform Computer Information Transactions Act, currently adopted as law in _____ and, effective ___, Virginia, is an effort to codify such transactions and create, among other things, a series of "default rules" regarding software licenses.

2. The Children's Online Privacy Protection Act of 1998, for example, 15 U.S.C. §§ 6501 *et seq.*, governs the online collection, distribution and use of

This article focuses on a particular kind of digital information–digitally encoded media such as music and movies–and the recently amended copyright law and related statues that protect that information. It is impossible to understand these statutes and regulations in a vacuum. They were passed with particular technologies and technological issues in mind against a background of an ongoing "battle" between large-scale copyright holders (primarily movie studios and record companies) and the unauthorized users of their intellectual property. Laws like the Digital Millennium Copyright Act (the "DMCA") and the Audio Home Recording Act of 1992 (the "AHRA") are fundamentally intertwined with the technological measures they describe and mandate. This article examines both the technologies and the laws that shape the present battle.

A copyright is a Constitutionally mandated, short-term monopoly on certain uses of a given work that is granted to its author "to Promote the Progress of Science and useful Arts."[3] A Constitutional mandate is necessary because the granting of exclusive rights of expression to one party necessarily entails the limitation of expressive conduct by others--a limitation that would otherwise run afoul of the First Amendment. Thus, the copyright laws must enact a delicate balance: On the one hand they must protect original works and create sufficient incentive for authors to create works for public consumption; on the other they must protect the public's rights of free expression and "society's competing interest in the free flow of ideas, information, and commerce." [4]

Each new media technology presents a new challenge to this

---

information regarding children under the age of 13.

3. U.S. Const. Art I, Sec. 8.

4. *Sony Corp. of America v. Universal City Studios,* 464 U.S. 417, 429 (1984). "The monopoly privileges that Congress may authorize are neither unlimited nor primarily designed to provide a special private benefit. Rather, the limited grant is a means by which an important public purpose may be achieved. It is intended to motivate the creative activity of authors and inventors by the provision of a special reward, and to allow the public access to the products of their genius after the limited period of exclusive control has expired." *Id.*

balance. The printing press was the impetus for the earliest British copyright protection;[5] the dire threat posed by the player piano roll gave rise to American copyright laws in 1908;[6] and the wide availability of high quality consumer audio recording equipment led to the passage of the Sound Recording Amendment of 1971.[7] "From its beginning, the law of copyright has developed in response to significant changes in technology. . . . Repeatedly, as new developments have occurred in this country, it has been the Congress that has fashioned the new rules that new technology made necessary."[8] Digital storage and distribution technologies present the most recent of these "new developments" and the major U.S. copyright holders have undertaken a war on two related fronts--technological and legal--to protect their valuable intellectual property.

Section II of this article focuses on the first front: technology. It describes the currently available forms of digital media and the technologies available for the compression, distribution and protection of those media. Section III describes the legal protections available to back up these technological measures (under the DMCA and other statutes) and examines in detail the most significant recent cases interpreting those statutes. The article concludes, in Section IV, with a discussion of where these legal and technological paths may eventually lead.

II. AN OVERVIEW OF DIGITAL MEDIA TECHNOLOGY

Generally, the term "digital" refers to a representation that consists of ones and zeros--the binary code understood by computers.[9] Its opposite, "analog," refers to phenomena that can have a range of values.[10] A dimmer is analog; an on-off switch is

5. *Id.* at 430.
6. *Id.* at 430 and n. 11.
7. Pub. L. No. 92-140, 85 Stat. 391(1971).
8. *Sony*, 464 U.S. at 430.
9. *Webster's New World Dictionary of Computer Terms* 160 (8th ed. 2000).
10. *Id.* at 25.

digital. Most real-world phenomena are fundamentally analog. The process of turning analog data into a digital representation that can be stored and manipulated by a computer is called digitization or encoding.[11] Any analog phenomenon can be digitized--an image,[12] a sound,[13] a movie or even a text file. Digitizing methods vary, but each accomplishes the same result: the creation of a string of ones and zeros that can be decoded and "played back" to reproduce the original analog experience.

A. The Advantages of Digital Technologies

Fundamentally, information must be in digital form to be stored in or manipulated by a computer or other digital device. However digital technology offers a variety of other benefits as well, including ease of duplication, electronic distribution, compression and encryption. The first three of these benefits combine to create new and potentially disastrous issues for copyright holders; the last may represent salvation.

1. Duplication

There is no way to make a perfect copy of an analog event. A photograph, sufficiently enlarged, will eventually show the grain of the photographic paper. A microphone, however sensitive, will always introduce a certain amount of "noise" into a recording. Digitizing an analog source also creates an imperfect (though often very good) copy. However, once the digital version is made it can

11. *Id.* at 163.

12. An image consists of subtle shades of color blending into one another; each color is a different frequency of light along the electromagnetic spectrum. This kind of variation along a spectrum is a good example of an analog phenomenon.

13. Sound, like color, is fundamentally analog. It consists of a complex waveform promulgated through air. Sound and color have ranges of value, they are not "on or off"—digital--phenomena.

be copied perfectly, from generation to generation without any loss of quality. For example, if I have a photograph of sunrise that I want to send to you, I might photocopy it and mail you the copy. The photocopy would be less clear than the original photograph, and if you decided to send a copy to your friend, your photocopy would be even less clear and so on until, twenty friends down the line, even the best color copiers would have reduced the image to a red and orange blur. This is because photocopying is an analog process. If, on the other hand, I had a digital copy of the sunrise image saved on my computer, I could email it to you, and you could email it whomever you liked and so on down the line. The twentieth copy of the file would be identical to mine, and so would the twenty thousandth.

There is no easy way to prevent this kind of perfect copying of digital media. Whatever the medium--CD, computer file, digital audio tape or DVD--the underlying information is nothing more than a string of ones and zeros, and that string of ones and zeros can always be copied verbatim by a computer equipped with the right software. If the underlying material is copyrighted, such copying may constitute infringement and there is substantial evidence that such digital trading in copyrighted material is widespread despite its illegality.[14] However, the cost of pursuing separate cases against each of the thousands of individual infringers who may have obtained copies of a work is simply too high to undertake. To prevent this kind of copying, copyright holders have turned instead to a number of other legal and technological strategies that concentrate on the source of the copies rather than the individual infringer.

2. *Compression*

Compression is the reduction of a digital file's size using a

14. *See, e.g., A&M Records, Inc v. Napster, Inc.*, 239 F.3d 1004, 1013 (9th Cir. 2001) (Plaintiffs demonstrated that more that at least 87% of the files on Napster's network were copyrighted and were being copied without permission by its users).

compression algorithm--a mathematical "recipe" that permits the removal of redundant or non-essential information.[15] The ease of making perfect copies of digital information would not, in itself, pose a serious threat to copyright holders if those copies could not be so easily distributed, but compression makes wide distribution a reality. Until the 1990s, for example, distribution of a digital copy of a CD--then the only consumer digital entertainment medium--meant burning a copy to a new CD or copying it to digital audio tape ("DAT") and selling it on the street or through other channels.[16] This kind of copying, though not especially widespread at the time, was perceived as enough of a threat that record companies lobbied hard for protection against it, resulting in the Audio Home Recording Act of 1992.[17]

Uncompressed multimedia files are extremely large. An average music CD weighs in at over 600 megabytes and a DVD movie at about five gigabytes.[18] Downloading such files over a standard modem simply is not practical; a single CD track would take well over two hours to download over a fast standard phone line, and a DVD would take over a week. However, recent advances in compression algorithms, combined with the increased availability of high speed Internet access to average households, have made

15. *Webster's New World Dictionary of Computer Terms* at 119.

16. In short, traditional, large-scale record piracy of the kind directly addressed by the Sound Recording Amendment as currently codified in the Copyright Law. 17 U.S.C. §§ 106(1)-(3), 106(6) & 114.

17. *See infra* at 17. The Audio Home Recording Act requires that certain consumer digital recording devices implement a system to prevent multiple generation digital copying and forbids creating or trafficking in devices designed to bypass that system. 17 U.S.C. § 1002(a), (c). It also requires the makers of digital recording devices to pay certain royalties to the RIAA to compensate record companies for the increased piracy risk. 17 U.S.C. § 1003.

18. *See, Universal City Studios, Inc. v. Reimerdes*, 111 F.Supp.2d 294, 313 (S.D.N.Y. 2000). DVD sizes vary, depending on the length of the movie and other factors, but the film data is usually well in excess of four gigabytes. *Id.* DVD is already a "compressed" format. Raw, uncompressed digital video data is much larger–roughly 20 megabytes *per second* at broadcast quality, or well over 100 gigabytes for a feature film. These sizes are prohibitive for any real-world application, and video is always compressed to some degree.

large scale distribution of digital multimedia files easier and more prevalent than ever. The most popular current technology for the compression of music files is the Moving Picture Experts Group's MPEG-1 audio layer 3 algorithm (commonly known as "MP3") while DiVX, a common video compression algorithm, is fast becoming a standard for video. MP3 is an "open" compression standard[19] that allows music files to be compressed to approximately one twelfth of their uncompressed size with no audible loss of quality.[20] DiVX, also an open standard, allows compression of a 5 gigabyte DVD into about 650 megabytes–small enough to be burned onto a recordable CD-R.[21] As a practical matter, this kind of compression, combined with the wide reach of the Internet and fast home access provided by technologies like cable-modems and DSL, means that pirated music (and, to a lesser extent, movies) are available to a much wider audience. An entire CD, converted to MP3, could be downloaded over a cable modem in approximately 20 minutes. A DVD compressed with DivX would still take a few hours to download over a fast home connection, but as consumer available bandwidth increases, that time is expected to drop considerably.[22]

---

19. An "open" standard or format is one that is non-proprietary and the technical specifications of which are freely available for user examination or modification. Anyone can implement an "open" standard without paying any license or other fees. *See, Webster's New World Dictionary of Computer Terms* at 386.

20. MP3 is an adjustable compression scheme that allows the user to sacrifice audio quality to reduce file size. At 12:1 compression most people consider the loss of audio quality negligible. *Webster's New World Dictionary of Computer Terms* at 358.

21. *Reimerdes*, 111 F.Supp.2d at 313-314. DivX was itself originally a "pirate" compression scheme (hence the anomalous capitalization). Microsoft's best video compression system, MPEG-4 v. 3, is only available in Microsoft's proprietary, encrypted "Advanced Streaming Format" video format which also includes rights management and copy protection features. DivX is a reverse engineered version of Microsoft's MPEG-4 v.3 implementation that is "open" and does not include any copyright protections. Trevor Marshal, *Open Source Video: The Web Video Turf Wars*, Byte.com, Sept. 11, 2000 (available at <http://www.byte.com/column/BYT20000905S0004>).

22. *Reimerdes*, 111 F.Supp.2d at 314.

Compression, large scale Internet distribution and the ease of making perfect digital copies combine to represent a serious threat to the rights of copyright holders. Large copyright holders such as the major motion picture studios and record labels have employed a two prong strategy to attack this new threat.[23] First, they have lobbied hard for new laws to protect their intellectual property rights from new digital threats and successfully tested these laws in court. Second, they have devoted their substantial resources to creating, marketing and supporting secure content delivery standards and systems that implement digital rights management. The cornerstone of this second prong is encryption technology.

3. Encryption

Encryption is "the process of converting a message into a ciphertext (the encrypted message) by using a key so that the message appears to be nothing but gibberish."[24] Encrypted data ordinarily cannot be read until it is decrypted using the appropriate key. However, no encryption system is perfectly secure and a sophisticated attacker can generally "break" any encryption scheme given adequate time and resources. There are countless

23. The music industry is often represented by its trade organization, the Recording Industry Association of America (the "RIAA") which "represents the roughly half-dozen major record companies (and the artists on their labels) that control approximately ninety percent of the distribution of recorded music in the United States." *Recording Industry Association of America v. Diamond Multimedia Systems, Inc.*, 180 F.3d 1072, 1074 (2d Cir. 1999) The movie studios are also represented by a trade organization, the Motion Picture Association of America (the "MPAA"), which serves as a "leader and advocate for major producers and distributors of entertainment programming for television, cable, home video and future delivery systems" and has on its board "the Chairmen and Presidents of the seven major producers and distributors of motion picture and television programs in the United States." MPAA Web Site (available at <http://www.mpaa.org/about>).

24. *Webster's New World Dictionary of Computer Terms* at 189. Encryption is distinct from encoding, which is the process described above of "digitizing," or creating digital versions of, analog data. *Id.* at 163.

schemes for encrypting data ranging from the simple to the complex, from the easily broken to the highly secure. For the purposes of this article it is only important to understand that digital data (including digitized audio and visual media files) can be encrypted by means that are well understood and commonly available so that they cannot be accessed by ordinary users without the permission of the person or company holding the encryption "key."

Encryption technology prevents all but the most sophisticated users from having unfettered access to the data on media they physically possess. As discussed in detail below, the paradigmatic present case is the DVD.[25] Movies distributed on DVD are protected by an encryption scheme called the Content Scrambling System ("CSS").[26] CSS (and more particularly, the CSS licensing system) prevents most consumers from making perfect digital copies of all or any portion of a movie stored on DVD.

Of course, encryption systems (including CSS) can be circumvented by someone of suitable skill, resources and motivation. This sort of circumvention is in itself a violation of the new anti-circumvention provisions of the copyright law put into place by the DMCA.[27] Trafficking in circumvention technologies or methods is also forbidden.[28] These new anti-circumvention and anti-trafficking provisions do *not* address infringement, however--the development and distribution of circumvention technology is forbidden whether or not such technology is actually used (or even useful) for an infringing purpose. This kind of law focuses on a lower level issue than the traditional copyright law: it bans the tools of copying (and the manufacture and distribution of those tools) rather than focusing on the copying itself, which may or may not be subject to other regulations. Thus encryption,

25. DVD (for "Digital Video Disk" or "Digital Versatile Disk") is "a CD-ROM format capable of storing up to a maximum of 17 GB of data, enough for a full-length feature movie." *Webster's New World Dictionary of Computer Terms* at 180.

26. *Reimerdes*, 111 F.Supp.2d at 309-10.

27. 17 U.S.C. §§ 1201 *et seq.*

28. 17 U.S.C. § 1201(a)(2).

combined with this kind of strong regulation, provides two kinds of protection: technological and legal. The technology itself prevents unfettered access by unsophisticated users, and the new anti-circumvention laws prevent sophisticated users from bypassing the technology.

B. The Current State of the Technology

Of the two major digital consumer entertainment formats in current use--DVDs for movies and CDs for music--the former is encrypted, and the latter is not. Content companies are pushing currently available technologies to their limits in search of a standard that will allow comprehensive, secure rights management for digital media without making millions of existing CD and DVD players obsolete.

1. DVDs and the Content Scrambling System

As noted above, the CSS encryption system for DVDs works two ways: as a technology, to prevent routine copying, and as a "technological measure that effectively controls access to a work" for purposes of the anti-circumvention provisions of the copyright law.[29] However, the real power of the CSS arises not from the copyright law, but from contract law. CSS is not an "open" encryption system, it is a proprietary encryption technology developed jointly by Matsushita Electrical Industrial Co. and Toshiba Corporation.[30] Matsushita and Toshiba licensed the technology to an industry trade group called the DVD Copy

29. 17 U.S.C. § 1201(a)(1)(A); *Reimerdes*, 111 F.Supp.2d at 317 ("CSS Effectively Controls Access to Copyrighted Works").

30. CSS License Agreement (V. 1.0) at Recital A (available, upon completion of forms, at <http://www.dvdcca.org/dvdcca/css/>). "Proprietary" in this case means that the patent on the technology and the copyrights on its implementations are owned by the corporations that developed them. One cannot legally implement CSS without a license from its owners.

Control Association (the "DVD-CCA") for purposes of administering CSS and licensing the technology to vendors and content creators.[31] If a manufacturer wants a CSS decryption "key" it must agree to the terms of the DVD-CCA license and pay certain fees to the DVD-CCA. The terms of the license--and thus the protections available to the copyright owner--are determined not by Congress, but by the members of the DVD-CCA. The DVD-CCA's membership includes all of the major motion picture studios, and the terms of the DVD-CCA license strongly reflect their input; the motion picture studios would not have agreed to release their DVD content encrypted with CSS unless they could be sure it was protected, and the DVD-CCA license accomplishes that end.

Thus, although I may purchase and own a DVD of *The Matrix*, my use of that DVD is, as a practical matter, limited to what the CSS license allows. For example, if I move to Japan, my U.S. copy of *The Matrix* will not work in my Japanese DVD player. Nothing in the copyright law creates this limitation--it is entirely a product of the CSS license provisions regarding "Region Encoding."[32] The CSS license also prevents any DVD player from being manufactured with direct, unprotected "digital outputs"[33]--manufacturers are prohibited from making a player that allows consumers to make a perfect, unscrambled digital copy of the movie data on the DVD. With this restriction in place, digital copying of DVDs is effectively impossible for the average consumer.

This kind of system, which relies on licensing and market dominance backed by strong anti-circumvention laws, allows

---

31. *Id.* at Recital B.

32. CSS Procedural Specification (V. 1.1), ¶ 6.2.1.4 (available, upon completion of forms, at <http://www.dvdcca.org/dvdcca/css/>). "Region Encoding" is a system of marking DVDs with codes representing the countries in which they can be played. Compliant DVD players check the region code to make sure the DVD is authorized for use in the country in which the player was purchased. A US DVD player will play only US authorized DVDs and not imports or resold foreign titles.

33. *Id.* ¶¶ 6.2.1.2 & 6.2.1.3

copyright holders to exert much finer control over their intellectual property than would be available under copyright law alone. The protections of the copyright law are very broad. They generally give authors the right to prevent most kinds of copying and other unlicensed use of their works--or at least the right to control such use and collect appropriate royalties. However there is nothing in the copyright law that permits an author to prevent a legitimate purchaser of her work from using it in another country. That restriction arises out of the DVD-CCA license alone and would not exist if not for that license.

Additionally, nothing in the copyright law prevents a professor from copying a short excerpt of a film for use in teaching a film class. That kind of copying is protected by the fair use exceptions that have so long been a part of the copyright law.[34] The CSS license prevents that kind of copying, however, and circumvention of CSS has recently been found to be a violation of the anti-circumvention provisions of the copyright law even if it is undertaken for proper, fair use purposes.[35] Alone, CSS is not a particularly powerful encryption system;[36] however acting in conjunction with the licenses and laws that support it, it provides copyright holders the means to apply very fine control over consumers' use of their intellectual property.

2. CDs and the Secure Digital Music Initiative

Unlike DVDs, CDs are not encrypted. Each track on a CD is an unencrypted digital file, and any consumer can simply place a CD in her computer's CD-ROM drive and have full, unfettered access to the music files stored on it. She can then easily copy, excerpt or modify those files, compress them into MP3 or other formats (a process called "ripping" the CD), burn them to a new CD or transmit them over the Internet like any other digital file. To the

34. *See* 17 U.S.C. § 107.
35. *Reimerdes*, 111 F.Supp.2d at 338.
36. *See supra* at n. 32.

computer, a music file on CD is no different from a word processing document or a digital photo.[37]

To address these issues, the music industry has once again turned to a technological standard called the Secure Digital Music Initiative ("SDMI").[38] SDMI is an effort to create a standard digital distribution format for music files that will tie certain kinds of copyright information and "usage rules" directly and permanently to the files themselves. This enables the holy grail of digital media distribution, comprehensive digital rights management ("DRM").

The proposed SDMI system consists of two parts: (i) a set of "rules" that all players (hardware or software) must follow if they wish to carry the "SDMI-Compliant" label; and (ii) a system for "watermarking" content–labeling digital music files with copyright information, "usage rules" and other rights management information.[39] SDMI-compliant players will read these usage rules from the watermark and apply them to the content. Contemplated usage rules include limitations on the number of copies that can be made, limitations on compressed copies, and even "expiration dates" or "counters" on individual songs, allowing users to download a song for a few days to decide whether to buy it.[40] Unlike CSS, the SDMI specifications are open, not proprietary, but like CSS they rely for their force on the market power of the participants, not the copyright law. Once the SDMI "Phase II" rollout is complete (an event that was scheduled for late 2000, but has been pushed back) only SDMI compliant players will be able

37. Of course, if the CD contains copyrighted materials, some of these activities might be prohibited by copyright law, but all would be simple as a technical matter. Most users can copy an move files on their computers and simple, easy to use software for editing music files and "ripping" MP3s from CD comes installed on most computers bought today.

38. The SDMI working group consists of representatives from the RIAA and other content providers, as well as hardware and software manufacturers. The SDMI Participant List is available at <http://www.sdmi.org/participant_list.htm>.

39. *SDMI Portable Device Specification*, Part 1, Version 1.0, July 8, 1999, ¶¶ 3.5, 3.7 & 10 (available at <http://www.sdmi.org/download/port_device_spec_part1.pdf>).

40. *Id.* ¶ 3.20.

to play SDMI watermarked content.[41] Because the RIAA, which controls ninety percent of the music released commercially in the United States,[42] is a member of the SDMI working group, it seems likely that most music (at least in this country) will soon carry the SDMI watermark. Every indication is that manufacturers of music players, both in the hardware and software worlds, are anxious to support SDMI in an effort to create a comprehensive DRM package for music.[43]

Like CSS, SDMI's watermarking and screening technologies are not perfect. SDMI issued a public challenge in September 2000 offering a reward to anyone who could remove the SDMI watermark from a sound file protected by one of five technologies, then under consideration for the final SDMI standard, without altering the file's sonic characteristics. SDMI awarded two $5,000 prizes to individuals who had defeated one of the five technologies in November 2000. The SDMI Working Group claims that the other four technologies remain secure.[44] However, a team of researchers from institutions such as Princeton, Xerox PARC, and

41. *Id.* ¶ 6.2.

42. See *supra* at n. 23.

43. DRM refers loosely to the ability to track and control (and thus charge for) content usage on a "per user" or even "per use" basis. This includes the ability to restrict the number of times a work can be played or copied, the kinds of users or machines that can access it, whether it can be given away or resold and whether it will eventually "expire", among other things. Microsoft's Windows Media Player ("WMP"), implements a full range of SDMI compliant DRM features. *WMP Rights Manager Technical Freatures and Benefits* (available at <http://www.microsoft.com/Windows/windowsmedia/en/wm7/RightsManager.asp>). Three of the five major U.S. record labels have also recently signed up to release their music on tiny optical discs the size of a quarter that hold up to 500 megabytes of encrypted data compressed in a format that allows each disc to hold five hours of music. The system includes DRM features that permit users to "unlock" the many albums that may be stored on each disc one at a time. *DataPlay Signs Content Deal With Music Label BMG*, PCWorld.com, Mar. 12, 2001 (available at <http://www.pcworld.com/news/article/0,aid,44102,00.asp>).

44. SDMI Press Release, *SDMI Awards Compensation to Successful Challengers*, Nov. 28, 2000 (available at <http://www.sdmi.org/pr/DC_Nov_28_2000_PR.htm>).

Rice disagree and claim to have cracked most or all of the potential SDMI watermarks.[45] The Princeton/Xerox/Rice team cancelled the scheduled reading of its paper on SDMI at a cryptography conference on April 26, 2001 due to the threat of a lawsuit by the RIAA and the SDMI Foundation based on the anti-circumvention provisions of the DMCA.[46] Regardless of whether SDMI is entirely secure or not, it functions in the same way CSS does: the technology prevents casual users from copying music and the anti-circumvention laws dissuade hackers from attacking the technology. The result is an environment that should provide a strong framework for complex DRM systems in the future.

III. THE LEGAL LANDSCAPE

The passage of the DMCA has extended the copyright law to include two very different kinds of legal protection for digital media: traditional infringement protections[47] and new, distinct anti-circumvention and anti-trafficking protections unrelated to infringement.[48] Traditional infringement protection is something of a "blunt instrument." A Copyright holder enjoys the following exclusive rights: (1) to reproduce the copyrighted work in copies or phonorecords; (2) to prepare derivative works based upon the copyrighted work; (3) 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; (4) in the case of literary, musical, dramatic, and choreographic works, pantomimes,

45. *Music Technology Forum Awards Hackers in Contest*, CNN.com, Nov. 29, 2000 (available at <http://www.cnn.com/2000/TECH/computing/11/29/hackers.reut/index.html>).

46. Such a suit is precisely the kind of chilling effect on legitimate research that critics worry may be the result of the recent decision in *Universal City Studios, Inc. v. Reimerdes*, 111 F.Supp.2d 294 (S.D.N.Y. 2000), discussed *infra* at 34-41. The paper at issue, and related materials including the RIAA/SDMI letter, are available at <http://cryptome.org/sdmi-attack.htm>

47. 17 U.S.C. § 106.

48. 17 U.S.C. §§ 1201.

and motion pictures and other audiovisual works, to perform the copyrighted work publicly; (5) 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 (6) in the case of sound recordings, to perform the copyrighted work publicly by means of a digital audio transmission.[49]

This statutory protection is broad, but as noted above it does not provide for much in the way of fine control over copyrighted materials of the kind contemplated by most DRM schemes. It also includes numerous "holes" arising, for example, out of the doctrines of "fair use,"[50] "first sale"[51] and even the statutory compulsory license.[52] However, as interpreted by the court in the

49. 17. U.S.C. § 106.

50. 17 U.S.C. § 107 ("Notwithstanding the provisions of sections 106 and 106A, the fair use of a copyrighted work, including such use by reproduction in copies or phonorecords or by any other means specified by that section, for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright"). Rather than attempt to list all fair uses, this section codifies the test for "fair use" created in the courts requiring an examination of "(1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes; (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and (4) the effect of the use upon the potential market for or value of the copyrighted work." *Id. See also* 17 U.S.C. 1201(c)(1) ("Nothing in this [anti-circumvention] section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title.").

51. 17 U.S.C. § 109(a) ("Notwithstanding the provisions of section 106(3), the owner of a particular copy or phonorecord lawfully made under this title, or any person authorized by such owner, is entitled, without the authority of the copyright owner, to sell or otherwise dispose of the possession of that copy or phonorecord."). A record label thus cannot prevent a purchaser of a CD, for example, from reselling that CD to another consumer. Copyright protection for a particular copy of a record, tape or CD thus generally ends with the "first sale" of that record, tape or CD.

52. 17. U.S.C. § 115(a) ("When phonorecords of a nondramatic musical work have been distributed to the public in the United States under the authority

only decision on the issue thus far, the anti-circumvention and anti-trafficking protections are not subject to these kinds of exceptions because circumvention and infringement are distinct offenses.[53] Thus, as the following cases make clear, there continues to be a role for traditional infringement cases in the digital world, but it is the combination of encryption technology and anti-circumvention protection that will no doubt dominate the digital copyright landscape.

A. Early Efforts: the Audio Home Recording Act and the Diamond Case

The DMCA is not the first effort to regulate digital copying through the copyright law. The Audio Home Recording Act of 1992 (the "AHRA")[54] was passed in response to recording industry concerns about Digital Audio Tape ("DAT"), then the only consumer recordable digital medium.[55] Rather than simply prohibiting the circumvention of protective technology generally, as the DMCA now does, the AHRA established a particular technological solution to the problem of multi-generational digital copying and enacted that solution into law. The AHRA specifies that any digital recording device subject to the Act must include an implementation of the Serial Copy Management System

---

of the copyright owner, any other person, including those who make phonorecords or digital phonorecord deliveries, may, by complying with the provisions of this section, obtain a compulsory license to make and distribute phonorecords of the work."). That is, once a musical work has been recorded and distributed, anyone can "cover" it subject to a statutory royalty–the author cannot prevent others from recording the work.

53. See, *Riemerdes,* 111 F.Supp.2d at 322.

54. 17 U.S.C. §§ 1001 et seq.

55. "Recording companies and creative artists believe that the precision of the digital audio recording capabilities will result in reduced sales and royalties due to illegal 'bootleg' copying, as well as home copying by consumers. They contend that this will, among other things, make it difficult for recording companies to introduce new artists and produce less popular recordings." H. R. Rep. 102-780, pt. 1, at __ (1992).

("SCMS")[56] or its equivalent. The AHRA also requires that manufacturers of digital recording devices pay certain royalties collectible by the RIAA[57] (to compensate for the increased risk of digital piracy) and forbids creating or trafficking in any device or service "the primary purpose or effect of which is to avoid, bypass, remove, deactivate, or otherwise circumvent" SCMS or its equivalent.[58]

SCMS is a technology that prevents multiple-generation digital copying from a protected source–that is, it prevents the making of "copies of copies."[59] It is not a true DRM system: it does not implement complex "usage rules."[60] For example, it allows any number of first generation copies to be made from a particular protected original. It does address what was, at the time, the major issue in large scale digital piracy: the making of a "chain" of perfect digital copies (and copies of copies) along a long distribution chain.[61] In that sense, the AHRA was quite narrowly targeted at a particular problem inherent in DAT and related technologies. When the RIAA attempted to extend the protection of the AHRA into the exploding area of MP3 distribution by suing a maker of MP3 players under the Act, it found that it could not do so.[62]

In *Recording Ind. Assoc. of America v. Diamond Multimedia*

---

56. 17 U.S.C. § 1002(a).

57. 17 U.S.C. § 1003.

58. 17 U.S.C. § 1002(c).

59. *Technical Reference Document for the Audio Home Recording Act of 1992, reprinted in* H.R. Rep. 102-780, pt. 1, at __ (1992).

60. See *infra* at 43.

61. "SCMS is intended to prohibit DAR devices from recording 'second-generation' digital copies from 'first-generation' digital copies containing audio material over which copyright has been asserted via SCMS. It does not generally restrict the ability of such devices to make 'first-generation' digital copies from 'original' digital sources such as prerecorded commercially available compact discs, digital transmissions of digital tapes." *Technical Reference Document for the Audio Home Recording Act of 1992, reprinted in* H.R. Rep. 102-780, pt. 1, at __ (1992).

62. *Recording Ind. Assoc. of America v. Diamond Multimedia Systems, Inc.*,180 F.3d 1072 (9th Cir. 1999).

Systems, Inc.,[63] the RIAA sued Diamond Multimedia, the maker of the popular Rio MP3 player, for failure to comply with the terms of the AHRA. The Rio is a small device, about the size of a cassette tape, that plays MP3s from its internal memory through a set of headphones.[64] It can store about an hour's worth of music (or up to two hours with an expansion card).[65] The only way to get MP3s into the Rio's memory is by transferring them from a home computer through a cable connected to the Rio.[66] The Rio, like most MP3 players, cannot record music directly, nor can it connect directly to the Internet; it can only load MP3s stored on a computer into its memory and play them as an analog audio signal, generally through headphones.[67]

The RIAA sought a preliminary injunction against the manufacture of the Rio, because the Diamond's software did not, at the time, include SCMS and Diamond was not paying the required royalty.[68] Upholding the District Court's denial of the preliminary injunction, the Ninth Circuit found that "the Rio is not a digital audio recording device subject to the restrictions of the Audio Home Recording Act of 1992."[69] This narrow holding--that the Rio simply is not the kind of device covered by the AHRA--was not particularly surprising. The AHRA defines a "digital audio recording device" as "any machine or device of a type commonly distributed to individuals for use by individuals, whether or not included with or as part of some other machine or device, the digital recording function of which is designed or marketed for the primary purpose of, and that is capable of, making a digital audio copied recording for private use . . . ."[70]

A "digital audio copied recording" is defined as "a reproduction in a digital recording format of a digital musical recording,

63. *Id.* at 1076-81.
64. *Id.* at 1074.
65. *Id.* at 1075.
66. *Id.*
67. *Id.*
68. *Id.* at 1073.
69. *Id.* at 1081.
70. 17 U.S.C. § 1001(3).

whether that reproduction is made directly from another digital musical recording or indirectly from a transmission."[71] To be subject to the AHRA, the Ninth Circuit found that a device must *either* (i) "record 'directly' from 'digital music recordings,'" or (ii) "make copies from transmissions."[72] The Court found that he Rio meets neither of these definitions because it can only get MP3 files from an attached computer and cannot record directly. Additionally, the Court held that "computers [and their hard drives] are not digital audio recording devices because their 'primary purpose' is not to make digital audio copied recordings."[73] A computer's hard drive generally contains substantial material other than, and unrelated to, the music.[74]

While seemingly a victory for Internet music distribution sites like Napster,[75] this finding has actually turned out to be a double-edged sword. The AHRA contains a provision making it explicitly *inapplicable* to taping for home use. It states, "No action may be brought under this title alleging infringement of copyright based on the manufacture, importation, or distribution of a digital audio recording device, a digital recording medium, an analog recording device, or an analog recording medium, or based on the noncommercial use by a consumer of such a device or medium for making digital musical recordings or analog musical recordings."[76]

In *A&M Records, Inc v. Napster, Inc.*,[77] Napster argued that its Internet music sharing service was used by consumers primarily for non-commercial, home use and that the service was therefore

71. 17 U.S.C. § 1001(1).

72. *Diamond*, 180 F.3d at 1076, 1081.

73. *Id.* at 1078. The District Court had rejected this interpretation, noting that it would create an enormous loophole in the protection afforded by the AHRA by allowing pirates to evade the AHRA simply by copying protected material to a computer before moving it to any other digital device. The Ninth Circuit agreed, but held: "While this may be true, the [AHRA] seems to have been expressly designed to create this loophole." *Id.*

74. *Id.* at 1076.

75. Napster is a web-based music trading community discussed in detail, *infra* at 27-33. Napster's home page is available at <http://www.napster.com>.

76. 17 U.S.C. § 1008.

77. 239 F.3d 1004 (9th Cir. 2001).

insulated from infringement liability by the AHRA.[78] The Ninth Circuit rejected the argument noting that plaintiff's claims did not arise under the AHRA and also that, under *Diamond*, even if Section 1008 of the AHRA were read more broadly, its protections would not apply to computer hard drives which are not covered by the AHRA.[79]

In the wake of the DMCA's much broader protection, the AHRA is essentially dead as an enforcement mechanism, but one final holding from *Diamond* bears mention. In support of its finding that the Rio should not be subject to the AHRA, the Ninth Circuit noted that "the Rio's operation is entirely consistent with the Act's main purpose--the facilitation of personal use."[80] Analogizing to the *Betamax* case,[81] in which the Supreme Court held that "time-shifting" copyrighted television programs by recording them for later viewing was a protected fair use. The *Diamond* Court held: "The Rio merely makes copies in order to render portable, or 'space-shift,' those files that already reside on the user's hard drive . . . Such copying is paradigmatic noncommercial personal use entirely consistent with the purposes of the Act."[82]

If the Ninth Circuit intended, by this analogy, to exempt all "space-shifting" copying from the Copyright Law on the grounds that such copying represents a fair use, this would be an extremely far reaching decision. For example, easy to use CD-ROM writers (or "burners") are available today to consumers at low cost and often include software to make digital "clones" of music CDs. May a user who has purchased a CD properly use her burner to make perfect digital copies of it for personal use in her car or office? *Diamond* appears to hold that such copying is no more objectionable than recording an episode of *ER* for later viewing.[83] The *Napster* decision, however, would seem to indicate that the

78. *Id.* at 1024.
79. *Id. (citing Diamond*, 180 F.3d at 1078).
80. *Diamond*, 180 F.3d at 1079.
81. *Sony Corp. of America v. Universal City Studios,* 464 U.S. 417 (1984).
82. *Diamond*, 180 F.3d at 1079 (*citing Sony Corp.*, 464 U.S. at 455).
83. *Id.*

Ninth Circuit does not endorse this reading, and will sharply limit *Diamond* to its facts.[84]

In any event, the RIAA has already shifted its focus. In the wake of the denial of its preliminary injunction, the RIAA dropped its suit against Diamond and issued a press release: "The RIAA is also pleased to bring a formal end to this legal process.... Today's announcement makes clear that the future of the digital music marketplace will be created in the marketplace itself, enabled by initiatives like SDMI."[85] Those initiatives, of course, are themselves enabled by the broad protections of the DMCA.

B. Traditional Infringement Actions

The strength of the DMCA's anti-circumvention protections has not entirely eliminated traditional infringement actions from the copyright holders' arsenal. As Judge Rakoff recently held in *UMG Recordings, Inc. v. MP3.COM, Inc.*, "[t]he complex marvels of cyberspatial communication may create difficult legal issues; but not in this case. Defendant's infringement of plaintiff's copyrights is clear."[86]

Record labels were empowered to bring these kinds of infringement actions by the Sound Recording Amendment of 1971.[87] Since the passage of that amendment, the copyright law has included certain limited protections for sound recordings themselves, as distinct from the traditional copyright protection

84. *Napster*, 239 F.3d at 1019 (*citing Diamond*, 180 F.3d at 1079).

85. *Diamond Multimedia, RIAA and AARC Settle AHRA Lawsuit,* RIAA Press Release, August 4, 1999 (available at <http://www.riaa.com/PR_Story.cfm?id=78>).

86. 92 F.Supp.2d 349, 350 (S.D.N.Y. 2000). In this case, discussed in detail *infra* at 23-6, defendant had converted several thousand of plaintiffs' most popular CDs into MP3s on its servers and was making them available to users who could prove they had previously purchased the CDs in another form. Judge Rakoff found that defendant had "copied" the CDs, for infringement purposes, by converting them to MP3s; thus his comment that infringement was clear, despite the complex technologies involved. *Id.*

87. Pub. L. No. 92-140, 85 Stat. 391 (1971).

afforded the songs being performed in the recording. Thus, the music on a CD is actually subject to at least two different copyrights: the copyright in the songs (and, sometimes separately, the lyrics) being performed, and the copyright in the particular recording of the performance. The song copyright is typically owned by the person who wrote the song. Each time the song is played on the radio the author is entitled to a statutory royalty.[88] The sound recording is also subject to copyright, and that copyright is typically held by the record label by contractual assignment from the artist, the studio personnel and others involved in the "authorship" of the recording.

The sound recording copyright is, by statute, a more limited copyright than the song copyright.[89] For example, the record labels are not permitted to collect statutory royalties for normal radio play of their records, but they are permitted to bring infringement actions against those who make copies of their records for wide distribution. It is not usually worthwhile for a copyright holder to pursue each individual infringer in cases of Internet or other wide area distribution. It is much more efficient to attack the root of the problem by pursuing those who create (or traffic in) encryption circumvention technology. However, in some cases a single infringer may be large enough--or central enough to the distribution chain--that an action for infringement (or vicarious or contributory infringement) may effectively be used against it.

1. MP3.com: The "Actual Infringement" Model

In some cases, an individual entity may be the source of "copies" for a large number of end users. This would be the case in a traditional pirate distribution chain in which a single music or video pirate makes thousands of copies of a recording and sells those copies to the public. The Sound Recording Amendment of

88. 17 U.S.C. § 115(a). In the U.S. these royalties are, for the most part, administered and distributed to the artists by the familiar royalty societies ASCAP and BMI.

89. *Compare* 17 U.S.C. §§ 106(4)-(5) *with* 17 U.S.C. §§106(6), 114.

1971[90] was passed to give record companies some recourse against this kind of copying. The *MP3.com* case[91] also involved large scale copying by a single entity, but it presented a uniquely Internet-based twist on the typical fact pattern.

MP3.com is a well known web site specializing in distributing music in MP3 form and providing information and support to the MP3 community. In January of 2000, MP3.com launched a new service called "My.MP3.com" designed to allow its users to access music they had bought on CD from any computer with an Internet connection.[92] My.MP3.com was essentially a universal Internet MP3 jukebox. MP3.com bought "tens of thousands of popular CDs," converted them to MP3 format, and stored the MP3s on its servers (or, as the court wrote "copied [plaintiffs'] recordings onto its computer servers").[93] MP3.com's subscribers could access the MP3 version of a given CD from any Internet--connected computer, but to do so they had to either (i) prove they owned the CD (by placing it in their CD-ROM drive for a few moments for reading by MP3.com) or (ii) purchase the CD from one of MP3.com's cooperating online retailers.[94] The point of the service was to provide the "functional equivalent" of a central jukebox containing all of the user's CDs (and nothing else--that is, no music the user had not properly purchased).[95] A number of record companies sued MP3.com in federal court in the Southern District of New York, charging that the My.MP3.com service constituted infringement on their sound recording copyrights. The District Court agreed, and granted plaintiff summary judgment on the issue of infringement.[96]

After rejecting, in a footnote, MP3.com's argument that converting the CDs to MP3 format for storage on a server did not

90. *See infra.*
91. *UMG Recordings, Inc. v. MP3.COM, Inc.*, 92 F.Supp.2d. 349 (S.D.N.Y. 2000).
92. *Id.* at 350.
93. *Id.*
94. *Id.*
95. *Id.*
96. *Id.* at 353

constitute "copying" under the copyright law,[97] the *MP3.com* court went on to address MP3.com's only substantial defense to infringement: fair use. The court examined each of the four statutory factors involved in determining whether a given use is protected as a fair use and found that all of them argued against a finding of fair use in this case.[98] The Court found (1) that MP3.com's copying was inherently commercial in nature;[99] (2) that the works being copied were creative works "close to the core of copyright protection";[100] (3) that then entire work was copied, and not merely a portion thereof;[101] and (4) that the copying harmed the record companies' ability to provide services similar to My.MP3.com and thus harmed the potential market value of their recordings.[102] MP3.com argued that its service merely provided space shifting on behalf of legitimate CD purchasers, and therefore constituted a protected fair use.[103] Without making any reference to the Ninth Circuit's holding in *Diamond*, the court rejected MP3.com's space shifting defense, calling it "simply another way of saying that the unauthorized copies are being transmitted in another medium."[104]

---

97. *Id.* at n. 1.

98. 17 U.S.C. §107 ("(1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes; (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and (4) the effect of the use upon the potential market for or value of the copyrighted work.").

99. *MP3.com*, 92 F.Supp.2d at 351.

100. *Id.* at 351-52.

101. *Id.* at 352.

102. *Id.* The District Court did *not* find that My.MP3.com harmed the market for CD sales–it could do so, because users of the service were required to prove they owned the CD prior to accessing the MP3s. Rather, the court found that the record companies have a separate right to provide a service similar to My.MP3.com (or to license their sound recordings to another such service) and that their sound recording copyrights include the right to make profit in that particular way, regardless of whether they presently do so.

103. *Id.* at 351. *See Diamond*, 180 F.3d at 1079 (*citing Sony Corp.*, 464 U.S. at 455).

104. *MP3.com*, 92 F.Supp.2d at 351.

Having found that the statutory factors[105] (as well as any other factors that might be relevant) argued against a finding of fair use, and after briefly considering MP3.com's other equitable defenses, the court granted plaintiffs' motion for summary judgment on the issue of infringement.[106] In the aftermath of the decision, MP3.com later reopened its service, this time as a "for pay" service under a licensing arrangement with the major music publishers.[107]

The MP3.com decision turned on the court's view that MP3.com was engaged in simple, old-fashioned piracy: the copying of plaintiffs' copyright material for defendant's commercial gain.[108] The fact that MP3.com had to "copy" CDs (by converting them to MP3 format and saving the resulting files on its servers) in order to run its service made the case a good fit for a traditional infringement analysis. In the world of digital distribution, however, cases are rarely so simple. For example, the *Napster* court faced a more complex question: can there be an action for infringement of CD music against a defendant who has not copied a single note?

---

105. *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 578 (1994) (Fair use analysis "is not to be simplified with bright-line rules, for the statute, like the doctrine it recognizes, calls for case-by-case analysis. The text employs the terms 'including' and 'such as' in the preamble paragraph to indicate the 'illustrative and not limitative' function of the examples given, which thus provide only general guidance about the sorts of copying that courts and Congress most commonly had found to be fair uses. Nor may the four statutory factors be treated in isolation, one from another. All are to be explored, and the results weighed together, in light of the purposes of copyright.") (citations and notes omitted).

106. *MP3.com*, 92 F.Supp.2d at 353.

107. *See Music Publishers and MP3.com Reach Preliminary Landmark Agreement*, MP3.com, Inc. Press Release, October 18, 2000 (available at <http://pr.mp3.com/pr/199.html>).

108. "Stripped to its essence, defendant's 'consumer protection' argument amounts to nothing more than a bald claim that defendant should be able to misappropriate plaintiffs' property simply because there is a consumer demand for it." *MP3.com*, 92 F.Supp.2d at 352.

2. *Napster: The "Vicarious or Contributory Infringement" Model*

In *A&M Records, Inc v. Napster, Inc.*,[109] the Ninth Circuit faced this exact issue. Napster is a file sharing and trading service that uses a slightly modified "peer to peer" network.[110] A user joins the Napster network by creating a user account and password at Napster's web site and designating a "user library" of files on her own computer that she wishes to share with others.[111] The user then downloads the Napster software and runs it on her computer.[112] When the user logs into the Napster network, the software does three things: (i) it informs Napster's central server that it is online and tells the Napster server what files are in its "user library;" (ii) it makes itself available to other computers for connection and downloading of those files; and (iii) it checks to see if any other available computers listed on the central Napster server have any files that its user wants.[113] The software can also transmit a search request to the Napster server to determine whether a particular file is available from any other connected user computer.[114]

If a user chooses to download a file from another user's computer, a "host," the Napster software gets the Internet address of the host from the Napster server, establishes a direct connection between the user and the host and deals with the technical details of file transfer.[115] The Napster server is, at that point, no longer a part of the equation and the user and the host continue to communicate directly with one another for the duration of the file

109. 239 F.3d 1004 (9th Cir. 2001).
110. *Id.* at 1011.
111. *Id.*
112. *Id.*
113. *See id.* at 1011-12.
114. *Id.* at 1012
115. *Id.*

transfer.

This description is something of an oversimplification and does not address all of the features of the Napster network,[116] but it is sufficient for purposes of this discussion to note that no computer owned or controlled by Napster contains copies of any portion of plaintiffs' copyright material. Rather Napster provides a central directory of it users, a list of files that users have made available for downloading and the software necessary to connect users together. There is no question that most of the files traded by Napster's users are MP3 files.[117] Napster's software is optimized for MP3 trading, it can play MP3s and in fact it confirms that the files being offered up by its users are MP3 files,[118] but Napster does not make copies of music as *MP3.com* did, so it cannot be liable for direct infringement.[119]

Instead, the plaintiff record labels and music publishers sued Napster seeking a preliminary injunction preventing Napster from continuing to offer its file trading services based on a theories of "contributory"[120] or "vicarious"[121] copyright infringement.[122] In

116. For a more detailed description, see *Napster*, 239 F.3d at 1011-13.

117. *Id.* at 1012.

118. *Id.* At the time of the injunction, the Napster software made sure that all the files in the user's "user library" listing were in MP3 format, but it made no attempt to verify what those files contained. File names were (and still are) supplied by the user with varying levels of descriptiveness and typographical accuracy. *Id.* As this article goes to press, Napster is changing its policies to conform to a new injunction that requires it to take stricter measures to prevent listing of copyright material.

119. *See id.* at 1013 (infringement occurs when a party "violate[s] at least one exclusive right granted to copyright holders under 17 U.S.C. § 106".)(*citing* 17 U.S.C. § 501(a)). As a general shorthand, violation of one of the five exclusive rights granted by 17 U.S.C. § 106 is often referred to as "copying." *Id.*

120. Contributory infringement arises when a party "'with knowledge of the infringing activities, induces, causes or materially contributes to the infringing conduct of another.'" *Id.* at 1019, *quoting Gershwin Publishing Corp. v. Columbia Artists Management, Inc.*, 443 F.2d 1159, 1162 (2d Cir. 1971). Contributory infringement was plaintiff's theory in the *Betamax* case. *Sony Corp.*, 464 U.S. at 434. ("The two respondents in this case do not seek relief against the Betamax users who have allegedly infringed their copyrights. . . . It is, however, the taping of respondents' own copyrighted programs that provides

Napster the Ninth Circuit granted plaintiffs a limited form of preliminary injunction based on the likelihood that plaintiffs would prevail on both of these issues, at least with respect to their own copyrighted material.[123]

To support a case for contributory or vicarious infringement, a plaintiff must first prove some underlying infringing use. In this case, the district court found that 87% of the music traded on Napster's network was copyrighted material and that at least 70% was material whose copyright was owned or administered by plaintiffs.[124] It also found that users' uploading and downloading of this music constituted infringement.[125] Napster apparently did not dispute that some users copied copyrighted material, but argued that such copying was protected under one of three categories of fair use: "sampling" (in which users download material to try it out before purchasing the CD), "space shifting" (which is described above), and authorized copying (in which artists, typically those without labels, release their music on Napster free of charge).[126]

Addressing each of the four statutory fair use factors, the court found that neither sampling nor space shifting constitute a protected fair use in the *Napster* context.[127] It upheld the district court's finding (i) that sampling is fundamentally a commercial

---

them with standing to charge Sony with contributory infringement. To prevail, they have the burden of proving that users of the Betamax have infringed their copyrights and that Sony should be held responsible for that infringement.").

121. Vicarious infringement is a more general theory arising out of the doctrines of "respondeat superior" and vicarious liability. *Napster*, 239 F.3d at 1022. It was not at issue in the *Betamax* case and has broader application than contributory infringement as it requires only that "defendant 'has the right and ability to supervise the infringing activity and also has a direct financial interest in such activities.'" *Id.* (*quoting Fonovisa, Inc. v. Cherry Auction, Inc.*, 76 F.3d 259, 262 (9th Cir. 1996)).

122. *Id.* at 1018, 1022.

123. *Napster*, 239 F.3d at 1027.

124. *Id.* at 1013.

125. *Id.* at 1013-14.

126. *Id.* at 1014. The court did not directly address the issue of authorized copying since it noted that plaintiff had not sought to enjoin such use and the injunction had not been crafted to capture it. *Id.* at 1019.

127. *Id.* at 1014-19.

use; (ii) that it involves the downloading of the entire work, (iii) that the works at issue are creative works close to the core protection of copyright; and (iv) that the downloading of songs for sampling purposes harms the commercial value of the copyrighted material.[128] As to this fourth fact, the *Napster* court found that, even if customers eventually buy CDs after downloading sample songs, the ability to "download a full, free and permanent copy of the recording" from Napster impairs the copyright holder's right to offer digital downloads of its own for sample purposes--including shorter excerpts of songs or entire songs programmed to "time out" after a given period.[129]

The Ninth Circuit also rejected the claim that Napster users were engaging in "space shifting" and that such use should be protected under *Diamond*.[130] The court distinguished Napster from the *Diamond* and *Betamax* "shifting" model based on Napster users' wide, public distribution of their files over the Internet.[131] The court held, "Both *Diamond* and *Sony* are inapposite because the methods of shifting in these cases did not also simultaneously involve distribution of the copyrighted material to the general public; the time or space-shifting of copyrighted material exposed the material only to the original user."[132]

Having found that Napster's users engaged in direct infringing behavior not protected by any fair use defense, the court went on to address the issues of Napster's liability under contributory infringement and vicarious infringement theories.[133] For its decision, the *Napster* court relied heavily on *Fonovisa, Inc. v. Cherry Auction, Inc.*,[134] an earlier Ninth Circuit decision in which a

128. *Id.* at 1018-19.

129. *Id.* at 1019. The Court wrote: "The record supports the district court's preliminary determinations that: (1) the more music that sampling users download the less likely they are to eventually purchase the recordings on audio CD; and (2) even if the audio CD market is not harmed, Napster has adverse effects on the developing digital download market." *Id.*

130. *See supra.*

131. *Napster*, 239 F.3d at 1019.

132. *Id.*

133. *Id.* at 1019-22

134. 76 F.3d 259 (9th Cir. 1996)

record label had sued an operator of swap meets[135] on theories of contributory and vicarious infringement. The court in *Fonovisa* found that the swamp meet operator was liable for contributory infringement because it had repeatedly been informed by the sheriff that its premises were being used to sell pirate records and "providing the site and facilities for known infringing activity is sufficient to establish contributory liability."[136]

The *Napster* court extended this analogy to Napster's software and service, finding that it materially contributed to direct infringement under the *Fonovisa* standard.[137] Napster argued that it was "nevertheless protected from contributory infringement by the teaching of *Sony Corp.*" in that its product was "capable of both infringing and 'substantial noninfringing uses.'"[138] The court addressed this issue in some detail and in fact wrote, "We depart from the reasoning of the district court that Napster failed to demonstrate that its system is capable of commercially significant noninfringing uses. The district court improperly confined the use analysis to current uses, ignoring the system's capabilities."[139] However, it found that "[r]egardless of the number of Napster's infringing versus noninfringing uses, the evidentiary record here supported the district court's finding that the plaintiffs would likely prevail in establishing that Napster knew or had reason to know of its users' infringement of plaintiffs' copyrights."[140]

Thus, the appellate court interpreted the *Betamax* test of "substantial noninfringing use" to be related entirely to the knowledge element of contributory infringement. That is, it found that the existence of substantial noninfringing uses for a

135. Swap meets are gatherings to which customers come to buy goods from independent vendors. The vendors rent booth space from the operator of the swap meet, and the operator supplies parking, conducts advertising and polices the area. The operator retains the right to deny vendors booth space for any reason at any time. *Id.* at 260.

136. *Id.* at 264.

137. *Napster*, 239 F.3d at 1022.

138. *Id.* at 1020, *quoting Sony Corp.*, 464 U.S. 417, 422.

139. *Id.* at 1021.

140. *Id.*

technology does not insulate the provider of that technology from liability, it merely makes it improper to "impute the requisite level of knowledge" to the provider for contributory infringement.[141] The number of noninfringing uses, the percentage of use that is noninfringing and other questions of amount and substantiality are thus irrelevant under the Ninth Circuit's reading: once any substantial noninfringing use is demonstrated, the question apparently becomes one of *actual* knowledge. In this case, the court found, the evidence established that Napster knew of, and indeed encouraged infringing use.[142] It wrote, "We agree that if a computer system operator learns of specific infringing material available on his system and fails to purge such material from the system, the operator knows of and contributes to direct infringement. Conversely, absent any specific information which identifies infringing activity, a computer system operator cannot be liable for contributory infringement merely because the structure of the system allows for the exchange of copyrighted material."[143]

The court also found that Napster faced liability for vicarious infringement, which arises where a defendant "has the right and ability to supervise the infringing activity and also has a direct financial interest in such activities."[144] Turning again to *Fonovisa*, the court found that Napster received a financial benefit from its users' infringement because "the availability of infringing material 'acts as a "draw" for customers.'"[145] Completing the analogy to the *Fonovisa* swap meet, the court also found that Napster had the ability to "control and patrol" its servers, ejecting users who trade in copyrighted material just as the swap meet organizer must

141. *Id.* at 1021-22.

142. *Id.* at 1022 ("The record supports the district court's finding that Napster has *actual* knowledge that *specific* infringing material is available using the system, that it could block access to the system by the suppliers of the infringing material, and that it failed to remove the material.") (emphasis supplied).

143. *Id.* at 1021 (internal citation omitted).

144. *Fonovisa*, 76 F.3d at 262.

145. *Napster*, 239 F.3d 1023 (*quoting Fonovisa*, 76 F.3d at 263-4).

police the aisles of the swap meet.[146] "Turning a blind eye to detectable acts of infringement for the sake of profit," the court wrote, "gives rise to liability."[147] The court noted, however, that the district court had "failed to recognize that the boundaries if the premises that Napster 'controls and patrols' are limited" and held that any injunction would have to be limited to acts Napster could be expected to take based on the file lists on its own servers, not its user's computers.[148]

In light of these findings on contributory and vicarious infringement (and after rejecting Napster's other arguments on waiver, implied license and copyright misuse), the Ninth Circuit remanded the case for entry of a new preliminary injunction. It directed that the new injunction require Napster to police its servers for the names of files that might indicate copyrighted material, and held that Napster and plaintiffs should share the burden of identifying plaintiffs copyright material listed on Napster's network.[149] Like *Diamond*, *Napster* is likely to be one of the last cases of its kind. The marketplace and encryption technologies have combined to make cases like *Napster* increasingly rare and even Napster itself, once the (alleged) darling of music pirates, is on its way to becoming part of the corporate structure of a major rights holder.[150]

146. *Id.* (*citing Fonovisa*, 76 F.3d at 261).

147. *Id.*

148. *Id.*

149. *Id.* at 1027.

150. *Bertelsmann and Napster Form Strategic Alliance*, Napster, Inc. Press Release, October 31, 2000 (available at <http://www.napster.com/pressroom/pr/001031.html>) ("Bertelsmann AG's newly formed eCommerce Group, BeCG, and Napster have developed a new business model for a secure membership-based service that will provide Napster community members with high-quality file sharing that preserves the Napster experience while at the same time providing payments to rights-holders, including recording artists, songwriters, recording companies and music publishers.").

C. Anti-Circumvention Actions

As the marketplace and industry move toward encryption technology, by far the most important new area of copyright enforcement will be the anti-circumvention lawsuit. The first of these is *Universal City Studios, Inc. v. Reimerdes*,[151] often referred to as the *DeCSS* case.[152] In the copyright context, *Reimerdes*' most important holdings are those regarding the possibility of fair use defenses to the anti-circumvention provisions of the DMCA.[153]

In *Reimerdes*, distributors of DVD motion pictures protected by CSS[154] sued Eric Corley, the editor of a magazine and website called *2600: The Hacker Quarterly*, seeking an injunction preventing him from publishing a program called DeCSS (and later, links to other web sites containing that program) on his magazine's web site.[155] DeCSS is a program, written for computers

151. 111 F.Supp.2d 294 (S.D.N.Y. 2000).

152. In fact, there are a number of cases relating to the DeCSS program including , No. CV 789804, 2000 WL 45812 (Cal. Superior Ct., Jan. 21, 2000), in which the DVD-CCA sought to prevent publication of the DeCSS or the CSS algorithm based on California trade secret law. The court enjoined the publication, but did not enjoin linking to other pages containing the information. *Id.* at *4. The case is presently stayed on jurisdictional grounds. *See*, *Pavlovich v. DVD Copy Control Association*, No. H021961 (Cal. Supreme Ct., Dec. 13, 2000) (unpublished, available at <http://www.eff.org/IP/Video/DVDCCA_case/20001213_ca_supct_order.html>). *Reimerdes* is the only DMCA anti-circumvention case in which there is currently an opinion.

153. Because the district court in *Reimerdes* ordered an injunction preventing any publication of the DeCSS source--and even any active hyperlink to any site containing the DeCSS code offered for purposes of dissemination–it spent a great deal of time addressing the First Amendment issues inherent in restraints of expressive speech. Although the district court's discussion of the expressive and functional qualities of computer code and hyperlinks is important in the First Amendment context, it is beyond the scope of this article.

154. *See supra* at 10-12.

155. *Reimerdes*, 111 F.Supp.2d at 308. Corley publishes the magazine under the pseudonym "Emmanuel Goldstein," a reference to the underground leader in George Orwell's *1984*. *Id.* Reimerdes and another defendant had already settled out by the time the case was heard and Corley was the only remaining defendant. The actual author or authors of DeCSS (including 15 year old Norwegian Jon Johansen, who gave testimony on Corley's behalf) were not

running the Windows operating system, "that enables uses to break the CSS copy protection system and hence view DVDs on unlicensed players and make digital copies of DVD movies".[156] Plaintiffs alleged that the publication of DeCSS violated Section 1201(a)(2) of the Copyright Act, an the DMCA's prohibition against trafficking in circumvention technologies, which states that:

> No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that:
>
> (A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title;
>
> (B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title; or
>
> (C) is marketed by that person or another acting in concert with that person with that person's

---

defendants in the case and apparently live outside the United States. *Id.* at 311. Corley may well have been chosen as a good defendant for this test case because many already considered him a criminal and "a leader of the computer hacker community" and because his magazine cultivates an "underground" image with the articles it publishes. *Id.* at 308-09. The choice was well made as the court made it very clear it had nothing but disdain for Corley and his magazine. *Id.*

156. *Id.* at 308. DeCSS is not a particularly easy program to use, nor is it very efficient. Many programs have come out since the publication of DeCSS that are faster, smaller and easier to use. Dr. David Touretzky, a Principal Scientist in the Computer Science Department at Carnegie Mellon University, maintains a fascinating "gallery" of DeCSS-like programs in many different forms, including the DeCSS code reproduced as art, DeCSS spelled out in ordinary English, DeCSS hand written in non-machine-readable form and several tiny programs short enough to be written on a cocktail napkin that accomplish the same thing as DeCSS. Touretzky, D. S., *Gallery of CSS Descramblers*, available at <http://www.cs.cmu.edu/~dst/DeCSS/Gallery>.

> knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title.[157]

The district court agreed with plaintiffs and, after addressing defendants First Amendment and fair use defenses, granted the injunction.[158] There is little question that the distribution of DeCSS is, under the strict statutory language, a violation of Section 1201(a)(2). The statute defines circumventing a technological measure as meaning "to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner."[159] A technological measure "effectively controls access to a work" under the statute, "if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work."[160] Under these definitions *any* encryption scheme, however simple, "effectively controls access to a work," and the *Reimerdes* court found that CSS fell within the statute's coverage.[161] Further, the court found that DeCSS was designed "primarily to circumvent CSS" and therefore constituted a circumvention technology prohibited by Section 1201(a)(1)(A).[162]

The district court also found that DeCSS did not fall into either Section 1201's extremely narrow statutory exceptions allowing the dissemination of circumvention technology for (i) reverse engineering research relating to interoperability;[163] (ii) some

157. 17 U.S.C. § 1201(a)(2). Section 1201(b) is substantially identical, except that it extends the same protection to any technology that "effectively protects a right of a copyright owner under this title" as opposed to one that "effectively controls access." 17 U.S.C. § 1201(b).

158. *Reimerdes*, 111 F.Supp.2d at 343-45.

159. 17 U.S.C. § 1201(a)(3)(A).

160. 17 U.S.C. § 1201(a)(3)(B).

161. *Reimerdes*, 111 F.Supp.2d at 318.

162. *Reimerdes*, 111 F.Supp.2d at 318-19.

163. 17 U.S.C. § 1201(f); *Reimerdes*, 111 F.Supp.2d at 319-320.

limited forms of encryption research;[164] or (iii) good faith security testing.[165] In addition to these three limited exceptions, the statute allows for some other exceptions as decided by the copyright office, none of which would have been relevant to the *Reimerdes* case.[166]

Having determined that none of the statutory exceptions were applicable, the district court went on to consider Corley's fair use defense. Corley argued that the statute should not apply to DeCSS because some copying of DVDs would constitute fair use.[167] The court agreed that "access control measures such as CSS do involve some risk or preventing lawful as well as unlawful use of copyrighted material."[168] It also noted, citing specific examples, that "technological means of controlling access to a copyrighted work may affect the ability to make fair uses of the work" and

---

164. 17 U.S.C. § 1201(g); *Reimerdes*, 111 F.Supp.2d at 320.

165. 17 U.S.C. § 1201(j); *Reimerdes*, 111 F.Supp.2d at 320.

166. The DMCA requires the Register of Copyright to conduct a rule-making process to examine the question of whether other exceptions to the anti-circumvention laws might be necessary to prevent trammeling fair use. 17 U.S.C. § 1201(a)(1)(B)-(C). The statute instructs Librarian of Congress to publish a list of users exempt from the primary anti-circumvention provision (though not the anti-trafficking provision) at the completion of that periodic rule-making. 17 U.S.C. § 1201(a)(1)(D). The rule-making had not been completed at the time of the *Reimerdes* decision, *Reimerdes*, 111 F.Supp.2d at 323 and n. 165, but if it had it would not have made any difference to the outcome, as neither of the two extremely limited exceptions arising from that process are relevant to DeCSS. The two classes of works identified by the Librarian of Congress as being exempt from anti-circumvention protection are: "(1) Compilations consisting of lists of websites blocked by filtering software applications; and (2) Literary works, including computer programs and databases, protected by access control mechanisms that fail to permit access because of malfunction, damage or obsoleteness." 37 C.F.R. § 201.40 (2000).

167. Apparently, Corley found this exemption in 17 U.S.C. 1201(c)(1) ("Nothing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title."). The court did not directly address this section, but its finding that there is no general statutory exemption for fair use suggests that it read this section to apply only to actions for *infringement* (that is, violations of Section 106), not actions for circumvention.

168. *Reimerdes*, 111 F.Supp.2d at 322.

pointed out that certain uses that would be "fair" for purposes of copyright infringement, including educational or artistic uses, "would be difficult or impossible absent circumvention of the CSS encryption."[169] Indeed, the court acknowledged that "as many have pointed out, technological means of controlling access to works create a risk, depending upon future technological and commercial developments, of limiting access to works that are *not* protected by copyright such as works upon which copyright has expired."[170]

However, the court found none of this determinative, however. It noted that Congress had struck a balance between protecting the proprietary rights of copyright holders and the fair use rights of individuals by crafting certain narrow exceptions into Section 1201 (as discussed above) and, more generally, by "limit[ing] Section 1201(a)(1)'s prohibition of the act of circumvention to the ac itself so as not to 'apply to subsequent actions of a person one he or she has obtained authorized access to a copy of the [copyrighted] work.'"[171] In other words, the *Reimerdes* court found that fair use need *not* apply as a defense to circumvention under Section 1201 because it does apply to any claim of infringement for subsequent use of the material, thereby protecting the rights of the fair users. This conclusion, however, may not be entirely borne out as a practical matter. The average "fair user" may never have a chance to engage in fair use copying of an encrypted digital source unless someone has first removed the encryption, thereby violating the anti-circumvention provision. Thus this reading greatly extends the effective protections of the copyright law: it makes any encrypted source subject to whatever rules the copyright holder may see fit to impose, rather than limiting its protections to the uses set out in Section 106.

Still, the court found that Congress had considered these issues and made up its mind. The court held, "The fact that Congress elected to leave technologically unsophisticated persons who wish to make fair use of encrypted copyrighted works without the

169. *Id.*

170. *Id.* at n. 159 (emphasis added) (citing, *inter alia*, David Nimmer, *A Riff on Fair Use*, 148 U.Pa. L.Rev. 673, 738-40 (2000)).

171. *Id.* at 323 (*quoting* H.R. Rep. No. 105-551, pt. 1, at 18 (1998)).

technical means of doing so is a matter for Congress unless Congress' decision contravenes the Constitution, a matter to which the Court turns below. Defendants' statutory fair use argument therefore is entirely without merit."[172]

Having found no statutory exception to the anti-circumvention law for fair users, the court turned the question of constitutionality. The court recognized that the DMCA does not create

> a notable potential impact on uses that copy portions of a DVD movie because compliant DVD players are designed so as to prevent copying. In consequence, even though the fair use doctrine permits limited copying of copyrighted works in appropriate circumstances, the CSS encryption of DVD movies, coupled with the characteristics of DVD licensed players, limits such uses absent circumvention of CSS. Moreover, the anti-trafficking provision of the DMCA may prevent technologically unsophisticated persons who wish to copy portions of DVD movies for fair use from obtaining the means of doing so.[173]

Nonetheless, on the facts before it, the court refused to hold unconstitutional the anti-circumvention and anti-trafficking provisions. It noted that the needs of fair users would be highly varied: some (such as the making of analog copies or transcripts of movies for study) might be served without circumventing CSS while others would not.[174] Given that, in its estimation, Corley's posting of DeCSS did not itself constitute a fair use, the court declined to consider the rights of "members of the 'fair use community'" *in bloc*; it held that, as applied to Corley, the DMCA

172. *Id.* at 323. The court also rejected defendant's fair use argument based on the *Betamax* case, noting that *Betamax* had concerned traditional infringement, not circumvention. *Id.*

173. *Id.* at 338 (footnote omitted). The court noted that the same problem might well arise with unprotected works or works whose protection has expired if those works are contained on encrypted media. *Id.* at n. 245.

174. *Id.*

is not unconstitutional and that Corley lacked standing to bring a constitutional overbreadth challenge on the behalf of potential fair users.[175]

The *Reimerdes* case is now on appeal to the Second Circuit and has garnered a great deal of attention from both sides of the issue. Rights-holders argue that these kinds of laws are necessary to give consumers the kind of seamless digital delivery of media and DRM that they demand. The United States government agrees, and the Department of Justice, recently filed a brief seeking the right to intervene on behalf of plaintiffs in the *Reimerdes* appeal.[176] *Amicus* briefs have also been filed on behalf of the studios by, among others, the RIAA, various actors', musicians' and authors' groups, various publishers and book, music and film marketers, Major League Baseball, the National Hockey League and the National Football League. On the other hand, a wide variety of interest groups object strenuously to *Reimerdes*' treatment of fair use rights (as well as the First Amendment ramifications of the decision) and there have also been numerous *amicus* briefs filed on behalf of Corley in his appeal by such diverse groups as computer scientists, law professors, cryptographers, members of the news media, the ACLU, librarians, authors and the Association for Computing Machinery.[177]

The reason for all this attention is that, in general, commentators, practitioners, and scholars read the decision to say that there is no fair use defense to the anti-circumvention and anti-trafficking provisions of the DMCA (which, in fact it does say) and that no such fair use defense is required to make the statute constitutional (which, as noted above, it does not quite say). For practical purposes, this amounts to a substitution of technology for law in the enforcement of the copyright bargain and that in turn tilts the bargain toward the rights of technically sophisticated copyright holders and away from the rights of fair users. David

175. *Id.* at 339.

176. All of the briefs in the *Reimerdes* appeal, including those of the parties, the *amici* and the United States, are available at <http://eon.law.harvard.edu/openlaw/dvd/>.

177. *Id.*

Nimmer writes, in his excellent article *A Riff on Fair Use in the Digital Millennium Copyright Act*:

> Historically, copyright owners have always had the right to retain their works confidentially.... Once those same owners consented to initial publication of the work, however, they have historically lost control over its subsequent flow. The first sale doctrine prevent them from barring or demanding a royalty upon subsequent disposition of published copies. The fair use doctrine prevented them from barring or demanding a royalty from such activities as miscellaneous quotations in the context of a review.[178]

Under the DMCA, however, "If copyright owners package their 'published' goods in digital envelopes accessible only through passwords, then perhaps they can, indeed, levy a unilateral royalty upon such activities as resales and reviews."[179] This sort of "pay per use" world is, opponents argue, not in keeping with copyright's Constitutional mandate "to Promote the Progress of Science and useful Arts" and constitutes an improper extension of the copyright monopoly to uses–and even entire classes of works–that would not normally be subject to protection.[180]

III. CONCLUSION

Under the copyright law, copyright holders have five exclusive rights in their works: (1) the right to copy them, (2) the right to prepare derivative works from them, (3) the right to distribute copies of them, (4) the right to perform them (if the works are

178. Nimmer, *A Riff on Fair Use*, 148 U.Pa. L.Rev. at 711.

179. *Id.* at 712.

180. *Id.* at 713-714 (noting that "pay-per-use" might extend to encrypted works whose copyright has expired or encrypted sources containing public domain material).

performance oriented), and (5) the right to display them publicly (if the works are display oriented).[181] These rights are limited by doctrines such as first sale and fair use.[182] These interlocking provisions create a complex balance in the copyright law--a balance between the need to protect rights-holders and the need to permit access to users. However, nothing in the copyright law allows a record company to sell a copy of a sample track from a hot album that expires after 48 hours. Nothing in the copyright law allows an artist to distribute a track that can be given away free as long as the recipient submits her name and address to a demographic tracking web site. Nothing in the copyright law allows a movie studio to sell DVDs that can be unlocked via credit card payment for one-time use. All of these innovations come from strong digital rights management technology and appropriate laws to back that technology.

The question then arises: what are the appropriate laws? In the copyright area Congress typically regulates conduct, not technology. It creates penalties for infringement, not for the creation of technologies that allow infringement. Cases like *Napster* and *MP3.com* show that traditional infringement actions still have substantial teeth, even within the limitations of *Betamax.* But the DMCA creates a new set of rights based directly on technology–the right to secure one's copyright behind a legally protected wall of encryption. In passing this law, at least as it has been interpreted in *Reimerdes*, Congress may have created a technological "loophole" that will eventually swallow the entire copyright bargain.

The protection of encryption, backed up by laws that offer no substantial exceptions for traditional fair use or first sale doctrines, negates, as a practical matter, the need to pursue any individual user on an infringement theory. The DMCA creates a strong incentive for all media to be distributed in encrypted form and,

181. 17 U.S.C. § 106(1)-(5). If the work is a sound recording, the owner loses the display and performance rights, but gains the exclusive right to "perform the copyrighted work publicly by means of a digital audio transmission". *Id.* § 106(6).

182. 17 U.S.C. §§ 107, 109(a).

despite its "Digital" name, even requires that all *analog* Beta, VHS and 8mm video tape devices carry access control systems subject to its anti-circumvention provisions.[183] Once encryption becomes the norm, the rights-holders, not Congress, will dictate what uses can and cannot be made of their properties. Thus far the dominance of "copyright-free" technologies like MP3 has prevented true DRM solutions from becoming widespread, but as more and more source material becomes encrypted the market will insist on players licensed to decrypt and play that source material, and the license terms will allow much finer control--and much greater flexibility--than the blunt instrument of traditional infringement could ever hope to achieve.

Consumers will certainly benefit from the legal and technological shift in the long run as more material becomes available in a more convenient forms, and the marketplace will eventually determine appropriate business models (even if the average savvy Internet user in 2001 is so used to getting her music free from *Napster* that she may be reluctant to pay at all). Unfortunately, it remains to be seen whether fair users--unwilling or unable to pay for the sources they need--will be a casualty of the digital distribution revolution.

183. 17 U.S.C. § 1201(k).